



**FACULTAD DE POSTGRADO
TRABAJO FINAL DE GRADUACIÓN**

**PROPUESTA DE MODELO PARA LA GESTIÓN DE
INCIDENTES DE SOFTWARE BASADO EN ITIL 4 PARA
BANCO FICENSA**

SUSTENTADO POR:

**ALEX GERARDO GÁMEZ ARTEAGA
RONALDO ENRRIQUE CÁRCAMO VÁSQUEZ**

PREVIA INVESTIDURA AL TÍTULO DE

**MÁSTER EN
GESTIÓN DE LAS TECNOLOGÍAS DE LA
INFORMACIÓN**

TEGUCIGALPA, FRANCISCO MORAZÁN, HONDURAS, C.A.

JUNIO, 2026

**UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA
UNITEC**

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTORA

ROSALPINA RODRÍGUEZ

VICERRECTOR ACADÉMICO NACIONAL

JAVIER ABRAHAM SALGADO LEZAMA

SECRETARIO GENERAL

ROGER MARTÍNEZ MIRALDA

DECANA FACULTAD DE POSTGRADO

ANA DEL CARMEN RETTALLY VARGAS

**PROPUESTA DE MODELO PARA LA GESTIÓN DE
INCIDENTES DE SOFTWARE BASADO EN ITIL 4 PARA
BANCO FICENSA**

**TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS
REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE**

MÁSTER EN

**GESTIÓN DE LAS TECNOLOGÍAS DE LA
INFORMACIÓN**

ASESOR METODOLÓGICO

JORGE RAÚL MARADIAGA CHIRINOS

ASESOR TEMÁTICO

MANUEL SALVADOR GARCÍA LACAYO

MIEMBROS DE LA TERNA:

CARLOS ROBERTO AMADOR

ALBA GABRIELA GARAY ROMERO

JUAN CARLOS ALMENDAREZ FLORES



FACULTAD DE POSTGRADO

PROPUESTA DE MODELO PARA LA GESTIÓN DE INCIDENTES DE SOFTWARE BASADO EN ITIL 4 PARA BANCO FICENSA

Alex Gerardo Gámez Arteaga
Ronaldo Enrique Cárcamo Vásquez

Resumen

La gestión de incidencias de software constituye un proceso crítico para la continuidad operativa del sector bancario, al influir en la calidad del servicio y en el control del riesgo tecnológico. El presente Trabajo Final de Graduación tuvo como propósito diseñar un modelo de gestión de incidencias de software basado en ITIL 4 para las áreas de Negocios y Operaciones de Banco FICENSA, orientado a mejorar la trazabilidad, reducir los tiempos de atención y resolución, y fortalecer el control operativo. La investigación adoptó un enfoque cuantitativo descriptivo, con diseño no experimental y transversal, utilizando datos correspondientes al año 2025. Se aplicaron tres instrumentos: un cuestionario de percepción, una matriz documental de incidencias y una matriz de evaluación de capacidad basada en COBIT 2019. Los resultados evidenciaron dispersión en los canales de reporte, incidencias gestionadas sin registro formal, tiempos prolongados de resolución y recurrencia de fallas en sistemas críticos. A partir de estos hallazgos, se propuso un modelo formal de siete etapas integrado a ManageEngine ServiceDesk Plus, acompañado de una matriz de criticidad, indicadores clave de desempeño y reglas de escalamiento. Se concluyó que el modelo propuesto representó una alternativa viable para fortalecer el gobierno de TI, reducir el riesgo operativo y elevar la madurez del servicio bancario.

Palabras clave: Banco FICENSA, COBIT 2019, gestión de incidencias, ITIL 4, gestión de servicios de TI.



GRADUATE SCHOOL

PROPOSAL FOR AN ITIL 4-BASED SOFTWARE INCIDENT MANAGEMENT MODEL FOR BANCO FICENSA

Alex Gerardo Gámez Arteaga
Ronaldo Enrique Cárcamo Vásquez

Abstract

Software incident management constitutes a critical process for the operational continuity of the banking sector, as it influences service quality and technological risk control. This Final Graduation Project aimed to design a software incident management model based on ITIL 4 for the Business and Operations areas of Banco FICENSA, focused on improving traceability, reducing response and resolution times, and strengthening operational control. The research adopted a descriptive quantitative approach, with a non-experimental and cross-sectional design, using data corresponding to 2025. Three instruments were applied: a perception questionnaire, a documentary incident matrix, and a process capability assessment matrix based on COBIT 2019. The results showed dispersion in reporting channels, incidents managed without formal registration, prolonged resolution times, and recurrence of failures in critical systems. Based on these findings, a formal seven-stage model integrated into ManageEngine ServiceDesk Plus was proposed, supported by a criticality matrix, key performance indicators, and escalation rules. It was concluded that the proposed model represented a viable alternative to strengthen IT governance, reduce operational risk, and increase the maturity of banking services.

Keywords: Banco FICENSA, COBIT 2019, incident management, ITIL 4, IT service management

DEDICATORIA

El presente trabajo de investigación se lo dedico primeramente a Dios, por darme la sabiduría, la fortaleza y la perseverancia necesarias para alcanzar este importante logro en mi vida.

De manera muy especial, dedico este triunfo a la persona más importante que tengo en mi vida: mi madre, Eva Arteaga. Gracias a su amor, apoyo, esfuerzo y enseñanzas, soy la persona que soy hoy en día. Ella ha sido mi mayor inspiración para seguir adelante, superar cada dificultad y luchar por mis sueños.

También dedico este logro a mi padre Mario Gámez, por su apoyo, por estar presente en mi vida y por brindarme la motivación necesaria para continuar avanzando. Su respaldo ha sido importante en este camino y forma parte de este triunfo que hoy alcanzo.

Alex Gerardo Gámez Arteaga.

Dedico este Trabajo Final de Graduación primeramente a Dios, por ser mi guía, fortaleza y fuente de sabiduría durante todo este proceso académico.

A mis padres y hermanos, por su amor, apoyo incondicional y por acompañarme en cada etapa de mi vida, motivándome siempre a seguir adelante y alcanzar mis metas.

De igual manera, dedico este logro a mi novia, Caroline Orellana, por su comprensión, sacrificio, paciencia y apoyo constante, especialmente en los momentos difíciles y por ayudarme a tener mi mejor versión.

Este logro representa también el respaldo, la fe y el cariño de quienes han sido parte fundamental de mi camino.

Ronaldo Enrique Cárcamo Vasquez

AGRADECIMIENTO

Primeramente, agradecemos a Dios, quien nos brindó la sabiduría necesaria para culminar este trabajo de investigación y nos dio la fortaleza para superar los momentos de dificultad que se presentaron durante este proceso.

Asimismo, expresamos nuestro agradecimiento a Banco FICENSA, por permitirnos desarrollar la investigación dentro de la institución y por brindarnos el espacio necesario para llevar a cabo este estudio.

De igual manera, agradecemos al personal docente de UNITEC, por la formación académica brindada durante el desarrollo de nuestra carrera y por contribuir significativamente a nuestro crecimiento profesional.

Agradecemos especialmente al Ph. D. Manuel Lacayo, nuestro asesor temático, por su orientación, conocimientos y guía durante el desarrollo de esta investigación. Asimismo, extendemos nuestro agradecimiento al Ph. D. Jorge Maradiaga, nuestro asesor metodológico, por su acompañamiento, apoyo y valiosas recomendaciones a lo largo de todo este proceso.

A todos ellos, nuestro más sincero agradecimiento por formar parte de este importante logro académico.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS.....	xviii
ÍNDICE DE GRÁFICOS.....	xix
ÍNDICE DE TABLAS	xxii
1. CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN	25
1.1. INTRODUCCIÓN	25
1.2. ANTECEDENTES DEL PROBLEMA.....	26
1.3. DEFINICIÓN DEL PROBLEMA	30
1.4. PREGUNTAS DE INVESTIGACIÓN.....	31
1.4.1. PREGUNTA GENERAL	31
1.4.2. PREGUNTAS ESPECÍFICAS.....	32
1.5. OBJETIVOS DEL PROYECTO	32
1.5.1. OBJETIVO GENERAL.....	32
1.5.2. OBJETIVOS ESPECÍFICOS.....	33
1.6. JUSTIFICACIÓN	33
2. CAPÍTULO II. MARCO TEÓRICO.....	35
2.1. MACROENTORNO.....	35
2.1.1. GESTIÓN DE SERVICIOS DE TI (ITSM)	35
2.1.1.1. DEFINICIÓN FORMAL Y ESTÁNDARES	35
2.1.1.2. ITSM COMO DISCIPLINA ESTRATÉGICA	36
2.1.1.3. EL MERCADO DE ITSM Y SU EVOLUCIÓN	36
2.1.1.4. IMPACTO EN EL SECTOR BANCARIO	38
2.1.2. EVOLUCIÓN DE ITIL COMO MARCO DE REFERENCIA EN GESTIÓN DE SERVICIOS	38
2.1.2.1. ITIL V2: ENFOQUE BASADO EN PROCESOS	40
2.1.2.2. ITIL V3: ENFOQUE BASADO EN EL CICLO DE VIDA DEL SERVICIO	41
2.1.2.3. ITIL 4: TRANSFORMACIÓN HACIA EL SISTEMA DE VALOR DEL SERVICIO	42
2.1.2.4. COMPARATIVA ENTRE VERSIONES	43
2.1.3. EL SISTEMA DE VALOR DEL SERVICIO (SVS)	45
2.1.3.1. LA CADENA DE VALOR DEL SERVICIO	46

2.1.3.2.	ENFOQUE HOLÍSTICO: LAS CUATRO DIMENSIONES.....	48
2.1.3.3.	MEJORA CONTINUA Y CO-CREACIÓN DE VALOR	50
2.1.4.	GESTIÓN DE INCIDENCIAS EN ITIL 4.....	51
2.1.4.1.	FLUJO OPERATIVO.....	52
2.1.4.2.	ROLES EN LA GESTIÓN DE INCIDENTES	53
2.1.4.3.	DIFERENCIAS ENTRE INCIDENTE, PROBLEMA Y CAMBIO.....	53
2.1.5.	LA MESA DE SERVICIO COMO FUNCIÓN ESTRATÉGICA	55
2.1.5.1.	DIFERENCIA ENTRE SERVICE DESK Y HELP DESK	55
2.1.5.2.	RELACIÓN CON LA CADENA DE VALOR DEL SERVICIO.....	56
2.1.5.3.	PLATAFORMAS ITSM: EL CASO DE MANAGE ENGINE	57
2.1.5.4.	MÉTRICAS E INDICADORES DE DESEMPEÑO (KPIs) EN GESTIÓN DE INCIDENCIAS	58
2.1.6.	INTEGRACIÓN MACROENTORNO	60
2.2.	MICROENTORNO	61
2.2.1.	CONTEXTO DEL SISTEMA FINANCIERO HONDUREÑO	61
2.2.1.1.	DIGITALIZACIÓN Y EXIGENCIAS OPERATIVAS	61
2.2.1.2.	PRESIÓN DEL ENTORNO REGULATORIO EN LA OPERACIÓN.....	62
2.2.1.3.	IMPLICACIONES PARA LA GESTIÓN DE INCIDENTES.....	62
2.2.2.	RIESGO TECNOLÓGICO EN EL SISTEMA FINANCIERO NACIONAL	63
2.2.2.1.	FRAUDES CIBERNÉTICOS Y AMENAZAS TECNOLÓGICAS.....	64
2.2.2.2.	DEPENDENCIA DE SISTEMAS CORE Y EXPOSICIÓN A INCIDENTES DE SOFTWARE.....	65
2.2.3.	CONTINUIDAD OPERATIVA EN INSTITUCIONES FINANCIERAS	66
2.2.3.1.	IMPACTO DE INCIDENTES DE SOFTWARE EN LA CONTINUIDAD OPERATIVA BANCARIA.....	66
2.2.3.2.	EFFECTOS OPERATIVOS DE INCIDENTES DE SOFTWARE.....	67
2.2.3.3.	CONTINUIDAD OPERATIVA Y RESTAURACIÓN DE SERVICIOS	67
2.2.3.4.	APLICACIÓN EN EL CONTEXTO INSTITUCIONAL: BANCO FICENSA 68	
2.3.	TEORÍAS DE SUSTENTO.....	69
2.3.1.	TEORÍA DE LA GESTIÓN DE INCIDENCIAS SEGÚN ITIL 4.....	70

2.3.2. TEORÍA DEL GOBIERNO CORPORATIVO DE TI	72
2.3.3. TEORÍA DE LOS INDICADORES CLAVE DE DESEMPEÑO (KPIS)	74
2.4. METODOLOGÍAS DESARROLLADAS	76
2.4.1. ITIL 4 (PRINCIPAL).....	76
2.4.1.1. JUSTIFICACIÓN DE LA ELECCIÓN DE ITIL 4.....	76
2.4.1.2. APLICACIÓN ITIL 4.....	77
2.4.2. COBIT 2019 (COMPLEMENTARIA).....	78
2.4.2.1. JUSTIFICACIÓN DE LA SELECCIÓN DE COBIT 2019	78
2.4.2.2. APLICACIÓN METODOLÓGICA DE COBIT 2019 EN LA INVESTIGACIÓN	81
2.4.3. INTEGRACIÓN ENTRE ITIL Y COBIT	82
2.5. INSTRUMENTOS UTILIZADOS.....	85
2.5.1. MANAGE ENGINE SERVICE DESK PLUS.....	85
2.5.2. COBIT 2019	87
2.5.2.1. MATRIZ DE EVALUACIÓN DE CAPACIDAD DEL PROCESO (COBIT 2019) 87	
2.5.2.2. MATRIZ RA DEL PROCESO DE GESTIÓN DE INCIDENCIAS DE SOFTWARE	87
2.5.2.3. INDICADORES CLAVE DE DESEMPEÑO (KPIS)	88
2.6. CONCEPTUALIZACIÓN.....	91
2.7. MARCO LEGAL.....	92
2.7.1. MARCO LEGAL NACIONAL	92
2.7.1.1. LEY DEL SISTEMA FINANCIERO (DECRETO NO. 129-2004)	92
2.7.1.2. COMISIÓN NACIONAL DE BANCOS Y SEGUROS (CNBS).....	94
2.7.1.3. RESOLUCIÓN NO. 025-2022 – NORMAS PARA LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD DEL NEGOCIO.....	96
2.7.1.4. RIESGO OPERACIONAL Y RIESGO TECNOLÓGICO EN EL SISTEMA FINANCIERO	97
2.7.1.5. GOBIERNO CORPORATIVO Y GESTIÓN DEL RIESGO TECNOLÓGICO EN EL MARCO REGULATORIO HONDUREÑO	99

2.7.1.6.	VINCULACIÓN DEL MARCO LEGAL CON LA PROPUESTA	100
3.	CAPÍTULO III. METODOLOGÍA DE LA INVESTIGACIÓN	101
3.1.	ENFOQUE.....	101
3.2.	ALCANCE.....	101
3.3.	DISEÑO DE INVESTIGACIÓN, POBLACIÓN Y MUESTRA.....	102
3.3.1.	DISEÑO.....	102
3.3.2.	POBLACIÓN.....	103
3.3.3.	TÉCNICAS DE MUESTREO	103
3.3.4.	MUESTRA	104
3.4.	CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN	105
3.5.	ESQUEMA DE VARIABLES	105
3.6.	OPERACIONALIZACIÓN DE VARIABLES	106
3.7.	TÉCNICAS, INSTRUMENTOS, PROCEDIMIENTOS Y PLAN DE ANÁLISIS ..	113
3.7.1.	TÉCNICAS.....	113
3.7.2.	INSTRUMENTOS.....	114
3.7.2.1.	CRITERIOS DE CLASIFICACIÓN Y CATEGORIZACIÓN DE INCIDENCIAS	115
3.7.2.2.	VALIDACIÓN Y CONFIABILIDAD DEL CUESTIONARIO	118
3.7.3.	PROCEDIMIENTOS.....	119
3.7.4.	PLAN DE ANÁLISIS.....	120
3.8.	FUENTES DE INFORMACIÓN	123
3.8.1.	FUENTES PRIMARIAS	123
3.8.2.	FUENTES SECUNDARIAS	124
3.9.	MATRIZ METODOLÓGICA	124
4.	CAPÍTULO IV. RESULTADOS Y ANÁLISIS.....	127
4.1.	INFORME DE PROCESO DE RECOLECCIÓN DE DATOS	127
4.2.	RESULTADOS Y ANÁLISIS	127
4.2.1.	ANÁLISIS CUESTIONARIO DE PERCEPCIÓN DE USUARIOS DE BANCO FICENSA	128
4.2.1.1.	SECCIÓN I. INFORMACIÓN SOCIODEMOGRÁFICA.....	129
4.2.1.2.	SECCIÓN II. HÁBITOS DE REPORTE ACTUALES	132

4.2.1.3.	SECCIÓN III. EVALUACIÓN DE PERCEPCIÓN Y SATISFACCIÓN.....	136
4.2.2.	ANÁLISIS DE LA MATRIZ DOCUMENTAL DE INCIDENCIAS DE SOFTWARE DEL AÑO 2025.....	162
4.2.2.1.	VOLUMEN TOTAL Y DISTRIBUCIÓN TEMPORAL DE INCIDENCIAS	163
4.2.2.2.	DISTRIBUCIÓN POR ÁREA FUNCIONAL.....	166
4.2.2.3.	DISTRIBUCIÓN POR SISTEMA AFECTADO	167
4.2.2.4.	DISTRIBUCIÓN POR TIPO DE INCIDENCIA	169
4.2.2.5.	DISTRIBUCIÓN POR MEDIO DE REPORTE Y TIPO DE REGISTRO....	172
4.2.2.6.	DISTRIBUCIÓN POR NIVEL DE CRITICIDAD	176
4.2.2.7.	ESTADO DE RESOLUCIÓN Y ANÁLISIS DE REINCIDENCIA	178
4.2.2.8.	ANÁLISIS INTERPRETATIVO DE POSIBLES CAUSAS RAÍZ POR SISTEMA	183
4.2.2.9.	ANÁLISIS DE TIEMPOS DE ATENCIÓN Y RESOLUCIÓN	185
4.2.2.10.	SÍNTESIS CUANTITATIVA DEL ANÁLISIS DOCUMENTAL	188
4.2.3.	EVALUACIÓN DE LA CAPACIDAD DEL PROCESO DE GESTIÓN DE INCIDENCIAS DE SOFTWARE BASADA EN COBIT 2019.....	191
4.2.3.1.	RESULTADO DE LA EVALUACIÓN DE CAPACIDAD DEL PROCESO	191
4.2.3.2.	ANÁLISIS DEL ESTADO ACTUAL AS-IS.....	195
4.2.3.3.	ESTADO OBJETIVO TO-BE Y BRECHA IDENTIFICADA.....	196
4.2.3.4.	IMPLICACIONES OPERATIVAS DE LA BRECHA.....	197
4.2.3.5.	SÍNTESIS DE LA EVALUACIÓN DE CAPACIDAD DE PROCESO.....	198
4.2.4.	INDICADORES CLAVE DE DESEMPEÑO (KPIS)	199
4.2.4.1.	RESULTADOS CONSOLIDADOS DE LA LÍNEA BASE.....	199
4.2.4.2.	PORCENTAJE DE INCIDENCIAS GESTIONADAS SIN REGISTRO FORMAL	200
4.2.4.3.	TIEMPO PROMEDIO DE ATENCIÓN	200
4.2.4.4.	TIEMPO PROMEDIO DE RESOLUCIÓN DE INCIDENCIAS (MTTR)	201
4.2.4.5.	TASA DE REINCIDENCIA	203
4.3.	HALLAZGOS PRINCIPALES	204

4.3.1.	ANÁLISIS DERIVADOS DE LOS RESULTADOS	204
4.3.2.	ANÁLISIS DE RIESGOS E IMPLICACIONES ESTRATÉGICAS DERIVADOS DE LOS HALLAZGOS	207
5.	CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES	211
5.1.	CONCLUSIONES	211
5.2.	RECOMENDACIONES.....	213
6.	CAPÍTULO VI. APLICABILIDAD	216
6.1.	NOMBRE DE LA PROPUESTA.....	216
6.2.	JUSTIFICACIÓN DE LA PROPUESTA.....	216
6.3.	ALCANCE DE LA PROPUESTA	218
6.3.1.	OBJETIVO GENERAL	220
6.3.2.	OBJETIVOS ESPECÍFICOS	220
6.4.	DESCRIPCIÓN Y DESARROLLO DE LA PROPUESTA	221
6.4.1.	POLÍTICA INSTITUCIONAL DE GESTIÓN DE INCIDENCIAS DE SOFTWARE	221
6.4.1.1.	SÍNTESIS ESTRUCTURADA DE LA POLÍTICA PROPUESTA.....	223
6.4.2.	FLUJO FORMAL DE SIETE ETAPAS DEL PROCESO DE GESTIÓN DE INCIDENCIAS	225
6.4.2.1.	ETAPA 1 - REGISTRO.....	226
6.4.2.2.	ETAPA 2 - VALIDACIÓN	231
6.4.2.3.	ETAPA 3 – CLASIFICACIÓN	236
6.4.2.4.	ETAPA 4 – PRIORIZACIÓN	242
6.4.2.5.	ETAPA 5 – ASIGNACIÓN.....	249
6.4.2.6.	ETAPA 6 - DIAGNÓSTICO Y RESOLUCIÓN.....	255
6.4.2.7.	ETAPA 7 - VALIDACIÓN DEL USUARIO Y CIERRE FORMAL	261
6.4.3.	MATRIZ DE CRITICIDAD, ACUERDOS DE NIVEL DE SERVICIO Y REGLAS DE ESCALAMIENTO	267
6.4.3.1.	MATRIZ DE CRITICIDAD.....	268
6.4.3.2.	MATRIZ DE ACUERDOS DE NIVEL DE SERVICIO	271
6.4.3.3.	REGLAS DE ESCALAMIENTO.....	272
6.4.3.4.	MATRIZ RA DEL PROCESO DE GESTIÓN DE INCIDENCIAS DE	

SOFTWARE	275
6.4.4. MAPA DE POLÍTICAS Y PROCESOS INSTITUCIONALES	278
6.5. MEDIDAS DE CONTROL	281
6.5.1. TABLEROS DE KPIs	281
6.5.2. CICLO DE CONTROL	284
6.5.3. ACCIONES ANTE DESVIACIÓN	285
6.5.4. ROLES DE SUPERVISIÓN DEL CONTROL	286
6.6. CRONOGRAMA DE IMPLEMENTACIÓN	288
6.7. PRESUPUESTO E IMPACTO DEL PRESUPUESTO	299
6.7.1. CONSIDERACIONES GENERALES DEL PRESUPUESTO.....	299
6.7.2. PRESUPUESTO ESTIMADO DE IMPLEMENTACIÓN	300
6.7.3. JUSTIFICACIÓN DEL PRESUPUESTO	301
6.7.4. ANÁLISIS FINANCIERO ESTIMADO DE LA PROPUESTA.....	302
6.7.5. BENEFICIOS ECONÓMICOS ESPERADOS	302
6.7.6. BENEFICIOS ECONÓMICOS ESTIMADOS POR CONTINUIDAD DE SOFTWARE	303
6.7.7. BENEFICIOS ESPERADOS POR MITIGACIÓN REGULATORIA	304
6.7.8. BENEFICIOS DE PROCESOS INTERNOS Y CUALITATIVOS	305
6.7.9. ESCENARIO DE RECUPERACIÓN DE LA INVERSIÓN A DOS AÑOS (ROI) 306	
6.7.10. CÁLCULO DEL RETORNO DE INVERSIÓN	306
6.7.11. PERÍODO DE RECUPERACIÓN DE LA INVERSIÓN	307
6.7.12. ANÁLISIS DE SENSIBILIDAD	307
6.7.13. COSTO DE OPORTUNIDAD DE NO IMPLEMENTAR EL MODELO	308
6.7.14. VIABILIDAD FINANCIERA DE LA PROPUESTA	309
6.8. CONCORDANCIA DE LOS SEGMENTOS DE LA TESIS CON LA PROPUESTA 310	
7. BIBLIOGRAFÍA.....	314
8. ANEXOS.....	317
ANEXO 1: MATRIZ DE EVALUACIÓN DE CAPACIDAD DEL PROCESO BASADA EN COBIT 2019	317

ANEXO 2: MATRIZ RA DEL PROCESO DE GESTIÓN DE INCIDENCIAS DE SOFTWARE	318
ANEXO 3: MATRIZ DE INDICADORES CLAVE DE DESEMPEÑO (KPIs).....	320
ANEXO 4: CUESTIONARIO DE PERCEPCIÓN DEL USUARIO	322
ANEXO 5: FORMATO MATRIZ DOCUMENTAL DE INCIDENTES DE SOFTWARE .	324
ANEXO 6: MATRIZ DOCUMENTAL DE INCIDENTES DE SOFTWARE CONSOLIDADA CON LAS INCIDENCIAS REGISTRADAS DURANTE EL AÑO 2025.	325
ANEXO 7: POLÍTICA INSTITUCIONAL DE GESTIÓN DE INCIDENCIAS DE SOFTWARE — BANCO FICENSA.....	329
ANEXO 8: INSTRUMENTO DE ENCUESTA AUTOMÁTICA DE SATISFACCIÓN POSTERIOR AL CIERRE.....	338
ANEXO 9: CARTA COMPROMISO ASESOR TEMÁTICO	340

ÍNDICE DE FIGURAS

Figura 1: Tamaño de mercado de las ITSMS a 2035.....	37
Figura 2: ITIL Framework V2	40
Figura 3: Estructura del ciclo de vida del servicio Itil V3	42
Figura 4: Historia de ITIL	44
Figura 5: El sistema de valor del servicio ITIL	46
Figura 6: Cadena de valor del servicio ITIL	47
Figura 7: Las cuatro dimensiones de la gestión de servicios	48
Figura 8: El modelo de mejora continua.....	51
Figura 9: Componentes del sistema de gobierno	79
Figura 10: Modelo Core de COBIT	82
Figura 11: Diagrama integrador de ITIL 4 y COBIT 2019	84
Figura 12: Logo ServiceDesk Plus	85
Figura 13: Versiones De ServiceDesk Plus De Manage Engine	86
Figura 14: Principios fundamentales de la regulación bancaria hondureña	94
Figura 15: Facultades de la Comisión Nacional de Bancos y Seguros.....	95

Figura 16: Estructura de gobierno en la gestión del riesgo tecnológico	100
Figura 17: Esquema de las variables del estudio	106
Figura 18. Relación de objetivos con instrumentos.	128
Figura 19. Tablero resumen de indicadores clave del análisis documental, año 2025.	190
Figura 20. Matriz de riesgos (mapa de calor) de la gestión de incidencias de software.....	209
Figura 21. Diagrama IPO, etapa 1	231
Figura 22. Diagrama IPO, etapa 2	236
Figura 23. Diagrama IPO, etapa 3	242
Figura 24.Evaluación del impacto operativo.	245
Figura 25. Evaluación de la urgencia técnica.	246
Figura 26. Cruce matricial impacto × urgencia.	247
Figura 27. Agravamiento por sistema crítico y activación del SLA.....	248
Figura 28. Diagrama IPO, etapa 4	249
Figura 29. Diagrama IPO, etapa 5	255
Figura 30. Diagrama IPO, etapa 6	261
Figura 31. Diagrama IPO, etapa 7	267
Figura 32. Sistema institucional de semaforización del cumplimiento del SLA.....	275
Figura 33. KPIs del modelo.	282
Figura 34. Borrador de tablero de KPI (Versión 1).	283
Figura 35. Borrador de tablero de KPI (Versión 2)	283
Figura 36. Ciclo de control del modelo.	285
Figura 37. Umbrales automáticos de activación ante desviaciones del tablero de KPIs.	286
Figura 38: Cuestionario Utilizado en Recolección de Datos	323

ÍNDICE DE GRÁFICOS

Gráfico 1: Género	129
Gráfico 2: Edad	130
Gráfico 3: Área a la que pertenece.....	131
Gráfico 4: Antigüedad en Banco Ficensa	132
Gráfico 5. ¿De qué forma escala las incidencias de software?	132

Gráfico 6: Actualmente, ¿Cuál es el medio que utiliza con mayor frecuencia para reportar una falla de software al departamento de TI?	134
Gráfico 7: ¿Con qué frecuencia suele reportar incidencias o fallas de software a TI?	135
Gráfico 8: ¿Cuál considera usted que sería el canal más adecuado para reportar incidencias de software?	136
Gráfico 9: El tiempo que tarda el departamento de TI en responder inicialmente a mi reporte de falla es rápido y adecuado.....	137
Gráfico 10: Generalmente, mis incidencias de software se resuelven en un lapso de tiempo que no interrumpe gravemente mis labores.	138
Gráfico 11: Cuando una incidencia afecta mis funciones diarias, siento que se le da la prioridad adecuada.....	139
Gráfico 12: En alguna ocasión he resuelto una falla de software por mis propios medios o con apoyo de un compañero, sin reportarla formalmente a TI.	140
Gráfico 13: Una vez que reporto una falla, recibo actualizaciones claras sobre el estado de mi solicitud sin tener que estar preguntando.....	141
Gráfico 14: Tengo claro cuál es el canal correcto para reportar una incidencia de software.	142
Gráfico 15: En ocasiones he tenido dudas sobre si mi incidencia fue realmente registrada o tomada en cuenta.....	143
Gráfico 16: La falta de un canal único dificulta dar seguimiento a las incidencias que he reportado.	144
Gráfico 17: El proceso actual descentralizado (usar Teams, correo o WhatsApp) para reportar problemas me resulta confuso o ineficiente.....	145
Gráfico 18: Un sistema centralizado de atención mejoraría la trazabilidad y control de las incidencias de software.	146
Gráfico 19: La existencia de varios canales para reportar incidencias (Teams, WhatsApp, Correo, etc.) me genera confusión.	147
Gráfico 20: He tenido que reportar la misma falla de software más de una vez en un período de 30 días.	148
Gráfico 21: Las soluciones brindadas por TI suelen ser definitivas y evitan que tenga que volver a reportar la misma falla poco tiempo después.	149
Gráfico 22: El personal de TI muestra disposición para atender los problemas reportados.	150

Gráfico 23: Las soluciones brindadas por TI suelen ser claras y fáciles de comprender.	151
Gráfico 24: Considero que el personal de TI tiene la capacidad técnica necesaria para resolver las incidencias de software que reporto.....	152
Gráfico 25: Cuando reporto una incidencia, generalmente logro indicar con claridad el nivel de urgencia o impacto que tiene en mis funciones.	153
Gráfico 26: Considero que el área de TI prioriza adecuadamente las incidencias según su nivel de criticidad para el negocio.	154
Gráfico 27: Cuando reporto una falla, suelo indicar si afecta a otras personas o áreas además de la mía.....	155
Gráfico 28: En términos generales, me encuentro satisfecho con la forma en que se gestionan actualmente las incidencias de software en Banco Ficensa.	155
Gráfico 29: El servicio que recibo por parte de TI cuando reporto incidencias de software cumple con mis expectativas.	156
Gráfico 30: Me siento confiado al reportar incidencias de software al área de TI porque considero que recibiré atención y seguimiento adecuados.	158
Gráfico 31: Considero que una Mesa de Servicio centralizada mejoraría la gestión de incidencias de software.	159
Gráfico 32: Utilizaría con frecuencia una Mesa de Servicio centralizada si estuviera disponible para reportar incidencias de software.	160
Gráfico 33: Considero que contar con un canal único y formal para reportar incidencias mejoraría mi experiencia de atención.	161
Gráfico 34. Distribución mensual de incidencias de software, año 2025	164
Gráfico 35. Distribución trimestral de incidencias de software, año 2025	165
Gráfico 36. Distribución de incidencias por área funcional, año 2025.....	166
Gráfico 37. Tasa de resolución de incidencias por área funcional, año 2025.....	167
Gráfico 38. Sistemas con mayor número de incidencias registradas, año 2025.	168
Gráfico 39. Distribución de incidencias por tipo, año 2025.	170
Gráfico 40. Tipo de incidencia según área funcional, año 2025.....	171
Gráfico 41. Distribución de incidencias por medio de reporte, año 2025.	173
Gráfico 42. Tipo de registro de las incidencias: formal vs. informal, año 2025.....	174
Gráfico 43. Tipo de registro según área funcional, año 2025.....	175

Gráfico 44. Distribución de incidencias por nivel de criticidad, año 2025.....	176
Gráfico 45. Nivel de criticidad según área funcional, año 2025.....	177
Gráfico 46. Estado de resolución de las incidencias, año 2025.....	179
Gráfico 47. Condición de reincidencia de las incidencias, año 2025.	180
Gráfico 48. Estado de resolución según condición de reincidencia, año 2025.....	181
Gráfico 49. Sistemas con mayor número de incidencias reincidentes, año 2025.....	182
Gráfico 50. Tiempo promedio de atención por área funcional, año 2025.	186
Gráfico 51. Tiempo promedio de resolución según nivel de criticidad, año 2025.	187

ÍNDICE DE TABLAS

Tabla 1: Comparación estructural de las versiones de ITIL	44
Tabla 2: Comparación conceptual entre incidente, problema y cambio	54
Tabla 3: Actores del entorno financiero hondureño	63
Tabla 4: Principales Tipos de Riesgos Tecnológicos Identificados en Honduras	64
Tabla 5: Incidentes de Software y su Impacto en Operaciones Bancarias	67
Tabla 6: Relación Entre Incidente de Software y Nivel de Impacto Operativo.....	68
Tabla 7: Elementos de Continuidad Operativa según Manual de Gestión de Tecnología.....	69
Tabla 8: Integración metodológica de ITIL 4 y COBIT 2019	83
Tabla 9: Comparación entre la Ley del Sistema Financiero y la Resolución No. 025-2022	98
Tabla 10: Criterios de inclusión y exclusión.....	105
Tabla 11: Operacionalización de variables descriptivas	108
Tabla 12: Vinculación Objetivos/Instrumentos	115
Tabla 13: Clasificación por Tipo de Incidencia.....	116
Tabla 14: Clasificación por Criticidad.....	116
Tabla 15: Clasificación por Medio de Registro	117
Tabla 16: Clasificación por Reincidencia	117
Tabla 17: Cálculo de Tiempos de Gestión.....	117
Tabla 18: Clasificación de Registro Formal	118
Tabla 19. Plan de Análisis Cuantitativo.....	122
Tabla 20: Matriz Metodológica	124

Tabla 21: Distribución de Incidencias por mes Año 2025.....	163
Tabla 22: Análisis interpretativo de posibles causas raíz por sistema	184
Tabla 23: Síntesis del análisis documental.	189
Tabla 24: Matriz de Evaluación de Capacidad del Proceso de Gestión de Incidencias de Software basada en COBIT 2019	192
Tabla 25: Síntesis de la Evaluación de Capacidad del Proceso	198
Tabla 26. Resultados consolidados de los indicadores clave de desempeño (KPIs).	199
Tabla 27: Hallazgos principales derivados del análisis de resultados	204
Tabla 28. Escala de valoración de la probabilidad.	207
Tabla 29. Escala de valoración del impacto.....	208
Tabla 30. Niveles de riesgo según la combinación de probabilidad e impacto.	208
Tabla 31: Riesgos e implicaciones estratégicas derivados de los hallazgos	208
Tabla 32. Beneficios cuantificables esperados de la implementación del modelo.	217
Tabla 33. Matriz de delimitación del alcance de la propuesta.	219
Tabla 34. Ficha de identificación documental de la política propuesta.	223
Tabla 35. Elementos de gobernanza, revisión y cumplimiento de la política.....	225
Tabla 36. Tiempos, responsables y puntos de control etapa 1.....	227
Tabla 37. Criterios objetivos de aceptación del dictamen de validación.	233
Tabla 38. Criterios objetivos de devolución o rechazo del dictamen de validación.	234
Tabla 39. Tiempos, responsables y puntos de control etapa 2.....	234
Tabla 40. Tiempos, responsables y puntos de control etapa 3.....	238
Tabla 41. CAT A. Catálogo oficial de Tipo de Incidencia.	240
Tabla 42. CAT B. Catálogo institucional inicial de sistemas afectados.	241
Tabla 43. CAT C. Catálogo de Tipos de vínculo con tickets previos.....	242
Tabla 44. Tiempos, responsables y puntos de control etapa 4.....	244
Tabla 45. Tiempos, responsables y puntos de control etapa 5.....	250
Tabla 46. Niveles de prioridad.....	252
Tabla 47. Mecanismos automáticos de reasignación de la Etapa 5.	253
Tabla 48. Tiempos, responsables y puntos de control etapa 6.....	257
Tabla 49. Tiempos, responsables y puntos de control etapa 7.....	264
Tabla 50. Nivel de impacto operativo.....	269

Tabla 51. Niveles de urgencia técnica.	269
Tabla 52. Matriz de impacto x urgencia.	269
Tabla 53. Sistemas reincidentes.	270
Tabla 54. Matriz SLA	271
Tabla 55. Reglas de escalamiento.	272
Tabla 56. Reclasificación de incidencias.	273
Tabla 57. Gestión de problemas por reincidencia.	274
Tabla 58. Roles en la matriz RA.	276
Tabla 59. Actores institucionales internos activados por escalamiento.	277
Tabla 60. Matriz RA del proceso.	277
Tabla 61. Mapa de políticas y procesos institucionales a actualizar según las conclusiones del estudio.	279
Tabla 62. Roles de supervisión de indicadores.	287
Tabla 63: Cronograma de implementación del modelo propuesto	289
Tabla 64: Resumen del cronograma de implementación	298
Tabla 65: Requisitos técnicos para la implementación de ManageEngine ServiceDesk Plus....	299
Tabla 66: Presupuesto estimado de implementación	300
Tabla 67: Supuestos económicos, regulatorios y de procesos internos para la estimación	303
Tabla 68. Beneficios económicos por continuidad de software.	304
Tabla 69. Beneficios de procesos internos y cualitativos.	305
Tabla 70. Recuperación de la inversión por año.	306
Tabla 71. Análisis de sensibilidad de la propuesta	307
Tabla 72. Costo de oportunidad de no implementar el modelo.	309
Tabla 73: Concordancia de los segmentos de la tesis con la propuesta.	311
Tabla 74: Concordancia entre objetivos específicos, hallazgos y componentes de la propuesta	312
Tabla 75: Formato de Matriz de Evaluación de Capacidad del Proceso Basada en COBIT 2019	317
Tabla 76: Formato de Matriz RA del Proceso de Gestión de Incidencias	319
Tabla 77: Formato de matriz de indicadores clave de desempeño (KPIs).	320
Tabla 78: Formato Matriz Documental de Incidentes de Software	324
Tabla 79: Síntesis de la matriz documental de incidencias de software, año 2025.	325

Tabla 80. Parámetros operativos del envío automático de la encuesta.....	338
Tabla 81. Escala Likert aplicable a los ítems evaluables.....	338
Tabla 82. Cuestionario base de la encuesta de satisfacción.....	338
Tabla 83. Umbrales institucionales de interpretación del CSAT.....	339

1. CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1. INTRODUCCIÓN

La presente investigación se refiere al tema de la gestión de incidencias de software en Banco Ficensa, específicamente en las áreas de Negocios y Operaciones, donde las incidencias asociadas al desarrollo de software no se gestionan mediante un sistema estructurado. Actualmente no existe un registro centralizado, la asignación al área de Desarrollo se realiza de forma informal, no se miden sistemáticamente los tiempos de atención y resolución ni se controla la reincidencia, lo que limita la trazabilidad del ciclo de vida de las incidencias y aumenta el riesgo operacional por fallas o indisponibilidad de sistemas críticos para el negocio.

El interés por abordar esta problemática surge de la necesidad institucional de fortalecer la gobernanza de TI mediante procesos formales, medibles y alineados con buenas prácticas internacionales, en un contexto bancario donde la continuidad operativa y la calidad del servicio son factores estratégicos. Para los autores, vinculados al campo de la Gestión de Tecnologías de la Información, resulta especialmente relevante disponer de un modelo que permita ordenar la atención de incidencias de software, reducir los tiempos de indisponibilidad de aplicaciones clave y mejorar la coordinación entre Negocios, Operaciones y Desarrollo de Software, generando además información confiable para la toma de decisiones.

En cuanto a la forma en que está pensado el trabajo, se plantea como un estudio de enfoque cuantitativo, de alcance descriptivo y diseño no experimental de corte transversal. El análisis se centrará en las incidencias de software registradas durante el año 2025, a partir de fuentes como correos electrónicos, reportes internos y bitácoras operativas, que serán consolidadas en una base de datos estructurada para calcular indicadores de frecuencia de incidencias, tiempos promedio de atención y resolución, porcentaje de incidencias gestionadas sin registro formal y tasa de reincidencia.

Estos resultados servirán de insumo para diseñar un flujo formal de registro, clasificación, escalamiento, seguimiento y cierre de incidencias alineado a la práctica de Gestión de Incidencias de ITIL 4, así como para definir indicadores clave de desempeño del servicio.

El estudio reconoce como limitaciones la dependencia de registros históricos que no fueron generados bajo un esquema estándar, lo que puede implicar datos incompletos o

inconsistentes, y la delimitación temporal al año 2025, que restringe el análisis a un periodo específico. Además, el ámbito de aplicación se circunscribe a las incidencias de software que afectan a las áreas de Negocios y Operaciones del Banco Ficensa, por lo que los hallazgos no pretenden generalizarse a otras instituciones ni a todos los servicios de TI del banco, y la propuesta se enfoca en la práctica de Gestión de Incidencias, dejando como líneas de continuidad futura la profundización en Gestión de Problemas, Gestión de Cambios y Gestión de Niveles de Servicio.

Para efectos de la presente investigación, se entiende por incidencia de software toda interrupción no planificada o degradación en la calidad de un servicio soportado por los sistemas de información desarrollados internamente por Banco Ficensa. Quedan excluidas de este concepto las incidencias asociadas a software comercial de terceros (COTS) y paquetes licenciados, así como las afectaciones de infraestructura, hardware, redes y telecomunicaciones. Esta delimitación obedece a que los sistemas objeto de estudio corresponden a desarrollos propios de la institución, sobre los cuales el área de desarrollo posee control directo del ciclo de vida del software y, por tanto, capacidad efectiva de intervención sobre las causas de las incidencias registradas

Con este marco, el objetivo general del Trabajo Final de Graduación es diseñar una propuesta de aplicación de la práctica de Gestión de Incidencias de ITIL 4 para la gestión de incidencias de software en las áreas de Negocios y Operaciones del Banco Ficensa, basada en el análisis de las incidencias registradas durante el año 2025.

1.2.ANTECEDENTES DEL PROBLEMA

A nivel internacional, la gestión de incidencias de tecnologías de información se ha consolidado como una práctica esencial dentro de los marcos de gestión de servicios de TI, en particular dentro del enfoque ITIL 4, debido al impacto que las interrupciones de sistemas ejercen sobre la continuidad del negocio y la calidad del servicio. De acuerdo con AXELOS (2019), la práctica de Gestión de Incidencias tiene como propósito “minimizar el impacto negativo de los incidentes restableciendo la operación normal del servicio lo antes posible”, asegurando que los niveles de calidad y disponibilidad acordados se mantengan.

Esta definición oficial establece la base conceptual para comprender la importancia de estructurar formalmente la atención de incidentes dentro de las organizaciones. La literatura científica señala que, ante la creciente digitalización de los procesos organizacionales, la ausencia de prácticas formales para la gestión de incidencias incrementa la probabilidad de interrupciones

prolongadas, afecta el desempeño operativo y limita la capacidad de las organizaciones para responder de manera eficiente a eventos no planificados (Ayala Soto & Caso Rojas, 2023).

Diversos estudios académicos coinciden en que la adopción de marcos de gestión de servicios de TI permite estructurar de manera sistemática la atención de incidencias, facilitando su registro, clasificación, priorización y seguimiento. En particular, la implementación de buenas prácticas basadas en ITIL 4 ha demostrado una influencia positiva en la reducción de los tiempos de atención y resolución de incidencias, así como en la mejora del nivel de satisfacción de los usuarios, al integrar enfoques ágiles y de mejora continua dentro de la gestión del Service Desk (Ayala Soto & Caso Rojas, 2023).

En este contexto global, sectores intensivos en tecnología como el financiero son identificados como especialmente sensibles a fallos en aplicaciones transaccionales, canales digitales y plataformas de atención. Ayala Soto & Caso Rojas (2023) confirman que la implementación de buenas prácticas basadas en el modelo ITIL 4 tuvo un impacto positivo en la gestión de servicios en el área de Service Desk de empresas de diversos sectores, lo que ha impulsado la adopción de soluciones de mesa de ayuda y software de gestión de servicios alineados con ITIL 4 para reducir interrupciones, fortalecer la continuidad operativa y responder a mayores exigencias regulatorias y de los clientes.

Banco Ficensa fue fundado el 26 de agosto de 1974 en Honduras, consolidándose como una institución financiera orientada principalmente al financiamiento del sector corporativo, caracterizada por una administración prudente del riesgo y la provisión de servicios financieros de alta calidad. En la actualidad, el banco cuenta con 14 agencias distribuidas estratégicamente a nivel nacional, lo que implica una operación descentralizada y altamente dependiente de sistemas de información para garantizar la continuidad de sus procesos de negocio.

Como entidad integrante del sistema financiero hondureño, Banco Ficensa desarrolla sus operaciones dentro del marco legal establecido por el Estado de Honduras y bajo la supervisión de los organismos rectores del sistema financiero, lo cual ha condicionado históricamente la forma en que la institución organiza y controla sus procesos operativos y tecnológicos. En este sentido, la Ley del Sistema Financiero (Decreto No. 129-2004) establece que su objetivo es “regular la organización, autorización, constitución, funcionamiento, función, conversión, modificación, liquidación y supervisión de las instituciones del sistema financiero y grupos financieros,

propiciando que éstos brinden a los depositantes e inversionistas un servicio transparente, sólido y confiable, que contribuya al desarrollo del país” (República de Honduras, 2004, pág. 2).

De manera complementaria, la Comisión Nacional de Bancos y Seguros (2022) , mediante las Normas para la Gestión de Tecnologías de Información, Ciberseguridad y Continuidad del Negocio (Resolución GRD No.793/16-12-2022), establece la obligación de que las instituciones supervisadas garanticen un Marco de Gestión de Tecnologías de la Información diseñado e implementado para asegurar la confidencialidad, integridad y disponibilidad de la información. Este marco normativo vigente actualiza las disposiciones históricas para adaptarlas a la rápida evolución tecnológica, exigiendo a las entidades financieras la documentación, monitoreo y gestión efectiva de sus procesos de TI, infraestructura y continuidad operativa.

Banco Ficensa es una institución financiera hondureña cuya operación depende de manera significativa del soporte de las Tecnologías de Información y Comunicaciones (TIC) para garantizar la continuidad de los procesos críticos. La creciente digitalización de los servicios financieros ha incrementado la necesidad de contar con procesos tecnológicos formales, documentados y alineados con la estrategia institucional. En este contexto, las áreas de Negocios y Operaciones dependen de manera directa de aplicaciones de software que soportan procesos críticos tales como la atención a clientes, la gestión de operaciones financieras y el cumplimiento de obligaciones regulatorias.

La indisponibilidad, fallas o retrasos en la atención de incidencias asociadas a dichos sistemas tienen un impacto inmediato en la eficiencia operativa de la institución y en la calidad del servicio brindado, además de poder incurrir en incumplimientos regulatorios.

De acuerdo con el Manual de Proceso de Gestión de Tecnologías de Información y Comunicaciones, la función de las tecnologías de información en Banco Ficensa tiene como propósito asegurar la disponibilidad, integridad y confiabilidad de los servicios tecnológicos que soportan la operación institucional, mediante la definición de procesos, responsabilidades y controles orientados a la adecuada gestión de los recursos de TI (Banco Ficensa, 2017).

En Banco Ficensa existe una mesa de servicio formal que gestiona una amplia gama de solicitudes e incidencias de TI mediante un sistema de tickets estructurado. Dentro de esta mesa de servicios existe un catálogo de servicios y acuerdos de nivel de servicio (SLA) definidos por tipo de ticket, categoría técnica, grupo responsable y prioridad, tal como se detalla en el

documento de acuerdos de nivel de Servicio IT (Banco Ficensa, 2024).

En dicho catálogo se contemplan, por ejemplo, tickets asociados a bases de datos, infraestructura, comunicaciones, soporte a usuarios y otros servicios técnicos, con tiempos de atención y resolución establecidos según la criticidad del requerimiento. No obstante, del análisis de dicho inventario de servicios se evidencia que las incidencias relacionadas con el desarrollo y funcionamiento del software que soporta a las áreas de Negocios y Operaciones no se encuentran contempladas dentro del esquema formal de atención de la mesa de servicio.

Como consecuencia, las incidencias de software son gestionadas mediante mecanismos no estandarizados, tales como correos electrónicos, comunicaciones directas o coordinaciones informales con el área de Desarrollo, lo que impide su registro centralizado, dificulta el seguimiento sistemático y limita la generación de información histórica confiable sobre su atención y resolución. La ausencia de un proceso formal para la gestión de incidencias de software genera múltiples ineficiencias dentro de la organización.

Entre las principales dificultades se identifican la falta de priorización adecuada de las incidencias, la imposibilidad de medir de manera objetiva los tiempos de atención y resolución, y la ausencia de indicadores de desempeño que permitan evaluar la efectividad del área de desarrollo en la atención de este tipo de eventos.

Quiñónez (2018) documentó una problemática similar en el Departamento de Tecnologías de Información de la Pontificia Universidad Católica del Ecuador Sede Esmeraldas, donde la falta de procesos estructurados para la gestión de incidencias generaba falta de informes sobre la resolución de incidentes, ausencia de integración entre la gestión de incidencias y otros procesos, y gestión deficiente de todos los incidentes reportados (Quiñónez Ku, 2018), situación que derivaba en pérdida de productividad, insatisfacción de usuarios y limitaciones para justificar presupuestos e inversiones en mejoras tecnológicas.

Esta situación configura, al mismo tiempo, una brecha de gestión y una oportunidad clara de mejora partiendo de que la organización ya dispone de un marco operativo, herramientas y experiencia previa en la implementación de una mesa de servicio con SLAs; por lo tanto, se encuentra en una posición favorable para incorporar, de manera estructurada y alineada con ITIL 4, la gestión de incidencias de software que afectan a las áreas de Negocios y Operaciones, cerrando así un vacío que actualmente limita la visión integral y la madurez de la gestión de

servicios de TI en el banco.

La necesidad de que las instituciones bancarias cuenten con procesos formales, documentados y controlados para la gestión de sus sistemas tecnológicos, incluyendo aquellos asociados al desarrollo y soporte de aplicaciones que impactan directamente en las áreas de Negocios y Operaciones. Abordar esta problemática resulta relevante en la medida en que una gestión estructurada de las incidencias de software contribuye a mejorar la eficiencia operativa, reducir los tiempos de indisponibilidad de los sistemas y fortalecer la continuidad de los servicios críticos del negocio.

Asimismo, la formalización de estos procesos permite generar información confiable para la toma de decisiones, mejorar la coordinación entre las áreas involucradas y disminuir el riesgo operativo asociado a fallas tecnológicas, lo cual repercute positivamente en la competitividad y sostenibilidad de la institución dentro del sistema financiero.

1.3.DEFINICIÓN DEL PROBLEMA

En el contexto actual del sistema financiero hondureño, los sistemas de información se han convertido en un pilar fundamental para la continuidad de las operaciones bancarias, la eficiencia de los procesos internos y la calidad del servicio que se brinda a los usuarios. Banco Ficensa, como institución financiera con presencia nacional y una operación distribuida en múltiples agencias, ha venido fortaleciendo su gestión tecnológica mediante la adopción de marcos normativos y procedimentales alineados a las disposiciones regulatorias vigentes y a buenas prácticas de gobierno de TI. Estos esfuerzos han permitido estructurar procesos formales para la administración de la infraestructura tecnológica, el soporte técnico a usuarios y la gestión del riesgo tecnológico.

Sin embargo, dentro de este entorno organizado, se identifica una brecha relevante en la forma en que se gestionan las incidencias relacionadas con el funcionamiento y desarrollo de software que afectan directamente a las áreas de Negocios y Operaciones. A diferencia de los incidentes asociados a infraestructura, redes o soporte al usuario final, que son atendidos mediante una mesa de servicio formal y acuerdos de nivel de servicio definidos, las incidencias de software no se gestionan a través de un esquema centralizado y estandarizado.

En la práctica, estos eventos suelen reportarse y atenderse de manera informal mediante

correos electrónicos, mensajes instantáneos o llamadas telefónicas, lo que genera dispersión de la información y dificulta su control.

Esta forma de gestión informal limita la capacidad del banco para contar con registros completos y confiables sobre las incidencias de software, afectando la trazabilidad de cada evento desde su reporte hasta su resolución en producción. Como consecuencia, resulta complejo medir de manera sistemática aspectos clave como la frecuencia de las incidencias, los tiempos promedio de atención y resolución, o la reincidencia de fallas en aplicaciones críticas. La falta de información consolidada reduce la posibilidad de analizar tendencias, identificar problemas recurrentes y tomar decisiones basadas en datos objetivos que contribuyan a la mejora continua de los servicios tecnológicos.

Adicionalmente, aunque el banco dispone de un subproceso formal orientado a la gestión y desarrollo del mantenimiento de sistemas, este se encuentra enfocado principalmente en cambios planificados y proyectos de desarrollo, sin cubrir de manera específica la atención operativa diaria de incidencias de software no previstas. En este contexto, la coordinación entre las áreas de Negocios, Operaciones y Desarrollo depende en gran medida de acuerdos informales y de la experiencia del personal, lo que incrementa el riesgo operativo y la probabilidad de retrasos o inconsistencias en la resolución de problemas que impactan procesos críticos del negocio.

Esta situación evidencia la necesidad de analizar de forma sistemática la gestión actual de las incidencias de software y de estructurar un modelo formal, trazable y medible, alineado a la práctica de Gestión de Incidencias de ITIL 4, que contribuya a mejorar la eficiencia operativa, reducir el riesgo tecnológico y fortalecer la continuidad de los servicios que soportan la operación de Banco Ficensa.

1.4.PREGUNTAS DE INVESTIGACIÓN

1.4.1. PREGUNTA GENERAL

¿Cómo puede diseñarse un modelo de gestión de incidencias de software desarrollado internamente, basado en la práctica de Gestión de incidencias de ITIL 4, a partir del análisis de la situación actual durante el año 2025, que permita mejorar la trazabilidad, reducir los tiempos de atención y resolución, y fortalecer el control operativo en las áreas de Negocios y Operaciones del Banco Ficensa?

1.4.2. PREGUNTAS ESPECÍFICAS

1. ¿Cuál es la situación actual de la gestión de incidencias de software desarrollado internamente en las áreas de Negocios y Operaciones de Banco Ficensa durante el año 2025, en términos de registro, trazabilidad, frecuencia de ocurrencia y control operativo de los casos reportados?
2. ¿Cuál es el tiempo promedio de atención y resolución de las incidencias de software desarrollado internamente registradas durante el año 2025 en Banco Ficensa?
3. ¿Cómo se clasifican y cuál es la distribución cuantitativa de las incidencias de software desarrollado internamente según tipo, criticidad y área afectada durante el año 2025 en Banco Ficensa?
4. ¿Qué porcentaje de incidencias de software desarrollado internamente fueron gestionadas sin registro formal durante el año 2025 en Banco Ficensa?
5. ¿Qué indicadores de desempeño deben establecerse para evaluar la gestión de incidencias de software desarrollado internamente del área de Desarrollo en Banco Ficensa?
6. ¿Cuál debe ser el flujo formal de registro, clasificación, escalamiento, seguimiento y cierre de incidencias de software desarrollado internamente en Banco Ficensa?

1.5. OBJETIVOS DEL PROYECTO

1.5.1. OBJETIVO GENERAL

- Diseñar un modelo de gestión de incidencias de software desarrollado internamente, basado en la práctica de gestión de incidencias de ITIL 4, a partir del análisis de la situación actual durante el año 2025, que permita mejorar la trazabilidad, reducir los tiempos de atención y resolución, y fortalecer el control operativo en las áreas de Negocios y Operaciones de Banco Ficensa.

1.5.2. OBJETIVOS ESPECÍFICOS

1. Analizar la situación actual de la gestión de incidencias de software desarrollado internamente en las áreas de Negocios y Operaciones de Banco Ficensa durante el año 2025, con base en el registro, la trazabilidad, la frecuencia de ocurrencia y el control operativo de los casos reportados.
2. Calcular el tiempo promedio de atención y resolución de las incidencias de software desarrollado internamente registradas en el año 2025 en Banco Ficensa.
3. Clasificar y cuantificar las incidencias de software desarrollado internamente según tipo, criticidad y área afectada durante el año 2025 en Banco Ficensa.
4. Determinar el porcentaje de incidencias de software desarrollado internamente gestionadas sin registro formal durante el año 2025 en Banco Ficensa.
5. Establecer indicadores de desempeño para evaluar la gestión de incidencias de software desarrollado internamente del área de Desarrollo en Banco Ficensa.
6. Definir un flujo formal de registro, clasificación, escalamiento, seguimiento y cierre de incidencias de software desarrollado internamente en Banco Ficensa.

1.6. JUSTIFICACIÓN

La presente investigación se justifica por la necesidad de fortalecer la gestión de las incidencias de software que afectan a las áreas de Negocios y Operaciones del Banco Ficensa, en un contexto donde la continuidad de los servicios tecnológicos resulta crítica para la operación del negocio bancario. Si bien la institución cuenta con procesos formales para la gestión de la infraestructura tecnológica y una mesa de ayuda con acuerdos de nivel de servicio definidos, la exclusión de las incidencias de software dentro de este esquema genera ineficiencias operativas, falta de trazabilidad y limitaciones para la toma de decisiones basada en información confiable.

La gestión informal de este tipo de incidencias dificulta el control de aspectos clave como la frecuencia de fallas, los tiempos de atención y resolución, y la reincidencia de problemas en aplicaciones críticas, lo que incrementa el riesgo operativo y puede afectar la calidad del servicio brindado a las áreas usuarias. En este sentido, la ausencia de un proceso estructurado limita la capacidad del banco para identificar oportunidades de mejora, priorizar adecuadamente los

recursos del área de desarrollo y evaluar de manera objetiva el desempeño de la gestión de servicios de desarrollo de software de TI.

Banco Ficensa, como entidad del sistema financiero hondureño, ha definido en su Plan Estratégico de Tecnologías de Información y Comunicaciones un conjunto de objetivos estratégicos orientados a mantener altos estándares de niveles de servicio y proveer infraestructura adecuada y de alta disponibilidad (Banco Ficensa, 2020). En particular, el objetivo estratégico OE3 establece como meta institucional "Mantener altos estándares de niveles de servicio dentro de la Gerencia de Tecnologías de Información y Comunicaciones" (Banco Ficensa, 2020, pág. 9), con un indicador de cumplimiento mínimo del 80% de satisfacción en la entrega de servicios de TIC a los usuarios de negocio.

Esta directriz institucional converge de manera directa con las buenas prácticas internacionales de gobernanza corporativa, al enlazarse con la meta de alineamiento AG05 del marco COBIT 2019, la cual exige la "Entrega de servicios de TI de acuerdo con los requisitos del negocio" (ISACA, 2018). En consecuencia, el cumplimiento de este indicador interno apoya de forma estructural el objetivo de gestión DSS02 de COBIT, enfocado en "Gestionar las peticiones y los incidentes del servicio". Por consiguiente, la formalización de un proceso para las incidencias de software resulta indispensable para operacionalizar dichas metas y asegurar la entrega de valor estratégico a la organización.

Desde el punto de vista institucional, la investigación resulta relevante porque propone una alternativa concreta y viable para integrar las incidencias de software dentro de un modelo formal de gestión alineado a la práctica de Gestión de Incidencias de ITIL 4, aprovechando la experiencia previa del banco en la implementación de una mesa de servicio con acuerdos de nivel de servicio. La propuesta que se derive del estudio permitirá mejorar la eficiencia operativa, reducir los tiempos de indisponibilidad de los sistemas, fortalecer la coordinación entre las áreas involucradas y contribuir a la mejora continua de la gestión tecnológica, generando valor tanto para la institución como para el sistema financiero en el que opera.

2. CAPÍTULO II. MARCO TEÓRICO

2.1.MACROENTORNO

2.1.1. GESTIÓN DE SERVICIOS DE TI (ITSM)

La Gestión de Servicios de TI (ITSM, por sus siglas en inglés) se comprende como una disciplina orientada a planificar, diseñar, entregar, operar y mejorar servicios de TI de forma que estos respondan de manera consistente a las necesidades del negocio y a las expectativas de los usuarios. En esta perspectiva, la TI deja de considerarse únicamente como un conjunto de componentes tecnológicos y pasa a gestionarse como un portafolio de servicios con objetivos, compromisos, mediciones y responsables.

Este enfoque resulta especialmente pertinente en organizaciones donde la operación depende de plataformas digitales y transaccionales; en tales contextos, la efectividad de la gestión de servicios no se evalúa por la existencia de infraestructura, sino por la capacidad de sostener niveles de servicio, responder ante interrupciones y controlar el riesgo asociado a la indisponibilidad.

2.1.1.1.DEFINICIÓN FORMAL Y ESTÁNDARES

Desde una perspectiva normativa, la norma ISO/IEC 20000-1:2018 —confirmada en su vigencia en 2023 y modificada mediante enmienda en 2024 para incorporar acciones relativas al cambio climático— especifica los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un Sistema de Gestión de Servicios (SGS), con el propósito de garantizar que la entrega de servicios de TI se encuentre alineada con las necesidades del negocio y cumpla con estándares de calidad medibles y auditables (Organización Internacional de Normalización, 2018).

La adopción de este estándar trasciende la mera corrección de fallos técnicos, pues su alcance radica en establecer un marco integral en el cual la tecnología es gestionada como un servicio que genera valor para la organización. En consecuencia, la implementación de las prácticas prescritas por la ISO/IEC 20000-1:2018 implica que la gestión de incidentes en el contexto de Banco FICENSA no constituirá una actividad reactiva y aislada, sino un proceso estandarizado, orientado a asegurar la calidad, la consistencia operativa y la mejora continua que la norma exige como condición para la certificación (Organización Internacional de

Normalización, 2018).

Este encuadre es relevante para la tesis porque el problema identificado en Banco Ficensa no se ubica en la ausencia de una herramienta de tickets, sino en la ausencia de un esquema estandarizado y trazable para registrar, priorizar, medir y controlar la atención de incidencias de software. ISO/IEC 20000-1:2018 establece requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de servicios (Organización Internacional de Normalización, 2018).

En un SGS alineado con ISO/IEC 20000, la gestión de incidencias se convierte en un mecanismo operacional que contribuye a mantener la continuidad del servicio y a asegurar que los compromisos del negocio se sostengan de manera medible, lo cual es coherente con el propósito de formalizar el ciclo de vida de las incidencias de software y generar evidencia histórica para decisiones de mejora.

2.1.1.2. ITSM COMO DISCIPLINA ESTRATÉGICA

Como disciplina, el ITSM trasciende la administración técnica de hardware o software. White (2019) explica que el ITSM consiste en políticas, procesos y procedimientos diseñados para planificar, entregar y soportar servicios de TI orientados al cliente. A diferencia de la gestión de tecnología tradicional, que se enfoca en los sistemas, el ITSM se centra en el cliente y en cómo la tecnología habilita los objetivos empresariales.

Para la gestión de incidencias, esta distinción es vital ya que por ejemplo un servidor caído no es solo un problema técnico, sino una interrupción en un servicio de negocio. Esta visión disciplina al equipo de soporte para priorizar las incidencias basándose en el impacto al negocio y no solo en la complejidad técnica, integrando marcos de trabajo como ITIL o COBIT para estructurar estas respuestas (White, 2019).

2.1.1.3. EL MERCADO DE ITSM Y SU EVOLUCIÓN

El ITSM también representa un mercado dinámico de herramientas y soluciones. Al Wazzan (2018) señala que la tecnología de la información se ha convertido en un recurso competitivo estratégico, donde la capacidad de procesar datos y conectar clientes con proveedores define la posición de mercado de una empresa. El mercado de herramientas ITSM (como ManageEngine, ServiceNow o Jira) ha evolucionado para soportar esta competitividad, ofreciendo plataformas que automatizan flujos de trabajo y centralizan el conocimiento.

Para esta investigación, el componente “mercado” no se aborda desde cifras de crecimiento, sino desde su implicación metodológica ya que la existencia de plataformas y enfoques industrializados de ITSM refuerza que el diseño propuesto para Banco Ficensa no es un ejercicio teórico aislado, sino una alineación con una forma estándar de operar servicios (registro, SLAs, medición, auditoría interna), especialmente útil cuando el banco ya dispone de una mesa de servicio implementada y, por tanto, de un punto de partida tecnológico y procedimental para incorporar incidencias de software en un esquema formal.

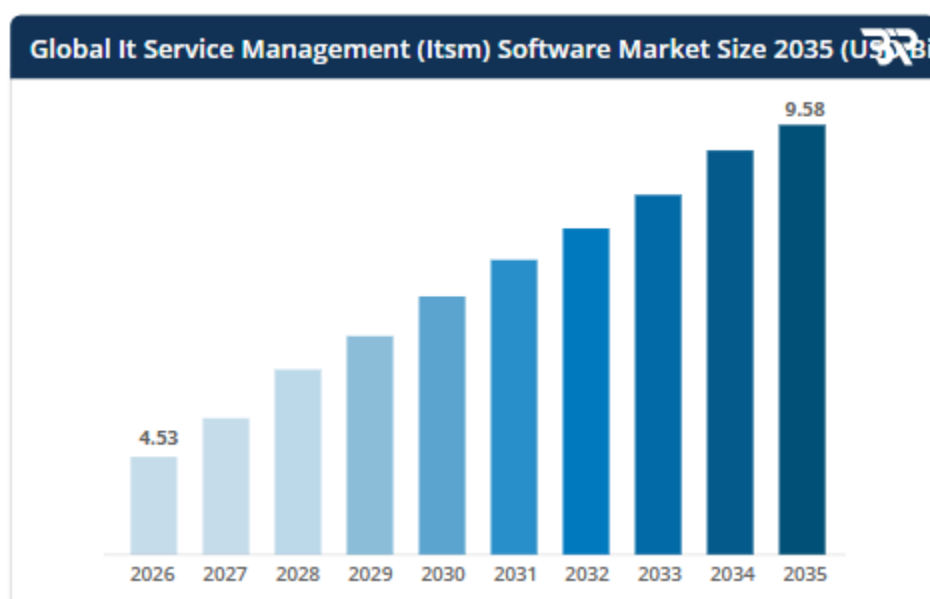


Figura 1: Tamaño de mercado de las ITSMS a 2035

Fuente: (Business Research, 2026)

El mercado mundial de software para la Gestión de Servicios de TI (ITSM) ha estado creciendo de forma sostenida en los últimos años y se espera que continúe expandiéndose de manera significativa en el futuro cercano. Varias investigaciones muestran que este mercado está valorado en varios miles de millones de dólares y que se espera que crezca a tasas compuestas anuales elevadas hasta aproximadamente 2030 – 2032.

Por ejemplo, uno de los análisis del tamaño del mercado global de ITSM indica que su valor podría aumentar de alrededor de USD 13,58 mil millones en 2025 a más de USD 36,7 mil millones para 2032, con una tasa de crecimiento anual de más del 15 % durante el período de pronóstico (MarketsandMarkets Research, 2025). Esto refleja la creciente adopción de soluciones

que ayudan a las organizaciones a planificar, diseñar, operar y administrar sus servicios de tecnología de manera más eficaz.

En la práctica bancaria, esto significa que la elección de una herramienta de Mesa de Ayuda no es una compra administrativa menor, sino una inversión estratégica. Una herramienta adecuada permite capturar datos sobre incidencias recurrentes, tiempos de respuesta y rendimiento del servicio, transformando la gestión operativa en inteligencia de negocios que puede guiar decisiones de inversión y mejora tecnológica (Al Wazzan, 2018).

2.1.1.4.IMPACTO EN EL SECTOR BANCARIO

La relevancia del ITSM en el sector bancario es crítica debido a la naturaleza de sus operaciones. Los bancos dependen intrínsecamente de sus sistemas de información para existir; en servicios financieros digitalizados, la organización es su tecnología (Al Wazzan, 2018).

- **Continuidad del Negocio:** La gestión de incidencias es la primera línea de defensa para la continuidad. Un incidente no resuelto rápidamente puede escalar a una crisis mayor que detenga las operaciones financieras. Un marco ITSM robusto asegura planes de recuperación y respuestas orquestadas ante interrupciones.
- **Riesgo Operacional:** La falta de procesos estandarizados aumenta el riesgo operacional. Si un incidente de seguridad o una falla de transacción no se gestiona con un proceso formal y trazable, el banco se expone a pérdidas financieras y de reputación. ITSM proporciona los controles necesarios para mitigar estos riesgos mediante la estandarización de la respuesta.
- **Regulación:** Los entes reguladores exigen a los bancos demostrar control sobre sus operaciones tecnológicas. La implementación de estándares como ISO/IEC 20000, facilitada por el ITSM, ofrece la evidencia de cumplimiento y gobernanza que los auditores requieren, validando que el banco gestiona sus activos tecnológicos de manera responsable y segura (Cots, 2011).

2.1.2. EVOLUCIÓN DE ITIL COMO MARCO DE REFERENCIA EN GESTIÓN DE SERVICIOS

La evolución de los marcos de referencia en gestión de servicios de tecnologías de información responde a la necesidad progresiva de estructurar, estandarizar y alinear la función

tecnológica con los objetivos estratégicos del negocio. Entre dichos marcos, ITIL® se consolidó como el referente internacional más adoptado para la gestión de servicios de TI, no como una norma prescriptiva, sino como un compendio de buenas prácticas adaptables a distintos contextos organizacionales.

ITIL® surge en la década de 1980 como resultado de una iniciativa impulsada por la Administración Pública del Reino Unido, en un contexto marcado por reformas orientadas a la externalización y privatización de servicios estatales. Ante la necesidad de establecer criterios homogéneos que permitieran evaluar y gestionar adecuadamente los servicios tecnológicos prestados por múltiples proveedores, el gobierno británico promovió la construcción de un marco de referencia basado en las mejores prácticas existentes.

Esta iniciativa, apoyada en experiencias previas del sector dio lugar a una biblioteca estructurada de buenas prácticas para la gestión de servicios de tecnologías de información, cuyo propósito fundamental era proporcionar un lenguaje común y una base metodológica compartida para la gestión de TI.

Desde sus fundamentos, ITIL se concibió como un marco orientado a la gestión de servicios y no exclusivamente a la gestión técnica de infraestructura. Esta distinción resulta fundamental, ya que introduce el concepto de IT Service Management (ITSM) como enfoque que entiende la tecnología no como un fin en sí mismo, sino como un medio para entregar valor al negocio a través de servicios estructurados.

Según AXELOS (2019) señala que ITIL constituye la guía más ampliamente adoptada para la gestión de servicios de TI a nivel mundial, consolidándose como un referente para organizaciones públicas y privadas de distintos sectores.

Un elemento distintivo de los fundamentos de ITIL es su carácter no prescriptivo. A diferencia de normas obligatorias, ITIL se presenta como un conjunto de buenas prácticas adaptables, lo que permite su implementación flexible según el tamaño, sector y madurez de cada organización. Esta característica explica su amplia adopción internacional, ya que puede coexistir con otros marcos de referencia, estándares y metodologías, tales como ISO/IEC 20000, COBIT o enfoques ágiles (AXELOS, 2019).

La evolución de ITIL puede comprenderse en tres grandes etapas estructurales: el enfoque

basado en procesos de ITIL v2, el modelo de ciclo de vida del servicio introducido en ITIL v3 y la transformación hacia el Sistema de Valor del Servicio (Service Value System) en ITIL 4. Cada versión refleja una adaptación a las dinámicas tecnológicas y organizativas de su tiempo, ampliando progresivamente la comprensión de cómo deben gestionarse las interrupciones del servicio dentro de un marco integral.

2.1.2.1. ITIL V2: ENFOQUE BASADO EN PROCESOS

La versión 2 de ITIL, consolidada entre los años 2000 y 2002 bajo la tutela de la Office of Government Commerce (OGC), tuvo como objetivo principal hacer más accesible la biblioteca de conocimientos sobre gestión de servicios de TI, reduciendo la colección original de más de 30 volúmenes a un conjunto más conciso de siete títulos organizados de forma lógica. A diferencia de la primera etapa, ITIL v2 estructuró la gestión en dos grandes dominios que fueron Service Support y Service Delivery, cada uno compuesto por procesos definidos con objetivos, actividades, entradas y salidas claramente especificadas (OGC, 2001).

El dominio Service Support incluía procesos como Gestión de Incidentes (Incident Management), Gestión de Problemas, Gestión de Cambios, Gestión de Configuración y Gestión de Versiones. Dentro de este conjunto, la Gestión de Incidentes adquirió especial relevancia al definirse como el proceso orientado a restaurar la operación normal del servicio lo antes posible y minimizar el impacto en el negocio (OGC, 2001).

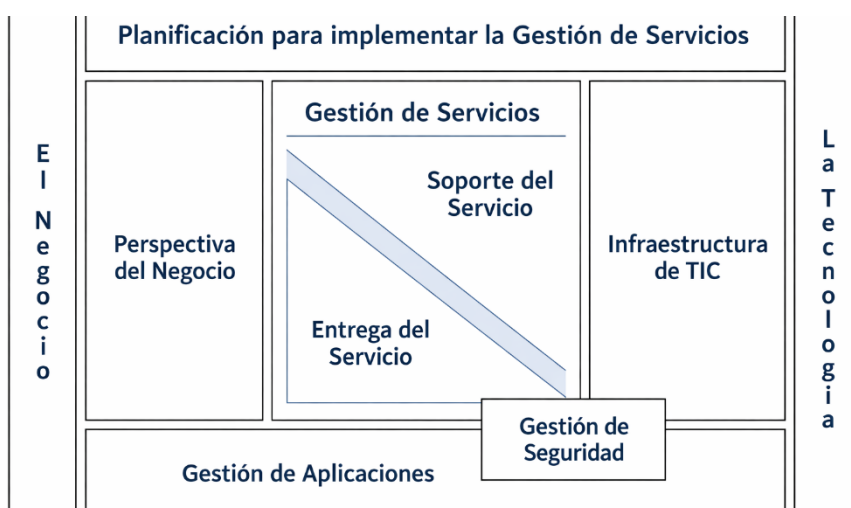


Figura 2: ITIL Framework V2

Fuente: (OGC, 2006)

El aporte de ITIL v2 a este estudio resulta relevante porque formaliza por primera vez la necesidad de gestionar incidentes bajo un esquema estructurado, trazable y medible.

2.1.2.2. ITIL V3: ENFOQUE BASADO EN EL CICLO DE VIDA DEL SERVICIO

La versión 3 de ITIL fue publicada oficialmente en 2007 por la Office of Government Commerce (OGC) del Reino Unido, como una evolución estructural significativa respecto a ITIL v2. Mientras que la versión anterior estaba organizada principalmente en torno a conjuntos de procesos operativos, ITIL v3 introduce una perspectiva integral basada en el ciclo de vida del servicio (Service Lifecycle), con el propósito de fortalecer la alineación estratégica entre las Tecnologías de Información y el negocio (OGC, 2011).

El marco de ITIL v3 se organiza en cinco etapas interrelacionadas, cada una documentada en una publicación central dedicada:

- Estrategia del Servicio (Service Strategy).
- Diseño del Servicio (Service Design).
- Transición del Servicio (Service Transition).
- Operación del Servicio (Service Operation).
- Mejora Continua del Servicio (Continual Service Improvement).

Según la propia publicación de *Service Strategy*, "el ciclo de vida del servicio utiliza un diseño de eje y radios (*hub-and-spoke*), con la estrategia del servicio en el centro, y el diseño, la transición y la operación del servicio como las etapas cíclicas o radios, mientras que la mejora continua del servicio rodea y soporta todas las etapas" (OGC, 2011, pág. 3).



Figura 3: Estructura del ciclo de vida del servicio Itil V3

Fuente: ITIL® Service Strategy

El cambio hacia el enfoque de ciclo de vida trajo consigo una visión integral en la que la gestión de servicios trasciende la mera administración de procesos operativos. ITIL v3 posiciona la gestión de servicios no solo como una "capacidad organizacional, sino como un activo estratégico" (OGC, 2011, pág. 5).

Diversos estudios empíricos han identificado factores de éxito y fracaso en la implementación de ITIL v3, señalando que su efectividad depende del compromiso directivo, la adaptación al contexto organizacional y la implementación gradual (Sánchez Casanova, 2021). Asimismo, se ha observado que una adopción excesivamente rígida puede generar burocratización y resistencia al cambio.

2.1.2.3. ITIL 4: TRANSFORMACIÓN HACIA EL SISTEMA DE VALOR DEL SERVICIO

ITIL 4, publicado en 2019, constituye la evolución más significativa del marco de referencia en sus más de 30 años de historia. A diferencia de las versiones anteriores, que se estructuraban en torno a procesos y al ciclo de vida del servicio, ITIL 4 introduce un enfoque holístico que "remodela gran parte de las prácticas ITSM establecidas en el contexto más amplio de la experiencia del cliente, los flujos de valor y la transformación digital, además de adoptar nuevas formas de trabajo, como Lean, Agile y DevOps" (AXELOS, 2019, pág. 2).

Los componentes clave de esta nueva versión son el sistema de valor del servicio (SVS)

y el modelo de cuatro dimensiones, los cuales proporcionan un marco flexible y adaptable para la gobernanza y gestión efectiva de los servicios habilitados por TI (AXELOS, 2019).

Este nuevo enfoque se articula principalmente a través del Sistema de Valor del Servicio (Service Value System, SVS) y de un conjunto de prácticas de gestión que sustituyen al catálogo tradicional de procesos, integrando aspectos como cultura organizacional, colaboración, tecnologías, información y relaciones con socios (AXELOS, 2019).

En lugar de concebir la gestión de servicios como una secuencia lineal de fases, ITIL 4 describe cómo múltiples actividades y recursos se combinan de forma flexible en flujos de valor que conectan la demanda y las oportunidades con la generación de resultados valiosos para clientes y organizaciones, apoyándose en principios rectores y en la mejora continua como elementos transversales (Anand, 2026).

2.1.2.4.COMPARATIVA ENTRE VERSIONES

La evolución del marco ITIL refleja un cambio progresivo desde una orientación técnica y operativa hacia una visión estratégica y de valor. Mientras que ITIL v2 (2000) se centró en la estandarización de procesos para el soporte y la entrega de servicios, e ITIL v3 (2007/2011) introdujo el concepto de ciclo de vida para alinear estos procesos con la estrategia del negocio, ITIL 4 (2019) rompe con la estructura lineal anterior para proponer un sistema flexible y multidimensional.

Historia de ITIL



Figura 4: Historia de ITIL

Fuente: PeopleCert

La Figura comparativa presentada anteriormente ilustra esta progresión estructural: ITIL v2 se organizó en dos grandes dominios (Service Support y Service Delivery), ITIL v3 consolidó 26 procesos distribuidos en cinco fases del ciclo de vida, y ITIL 4 adoptó 34 prácticas integradas dentro del SVS y la cadena de valor del servicio (Anand, 2026).

Tabla 1: Comparación estructural de las versiones de ITIL

Característica clave	ITIL v2 (2000-2007)	ITIL v3 / 2011 (2007-2019)	ITIL 4 (2019 - Presente)
Enfoque principal	Procesos de TI	Ciclo de vida del servicio	Sistema de Valor del Servicio (SVS)
Estructura central	Dominios principales: - Service Support. - Service Delivery.	5 fases del ciclo de vida: - Estrategia - Diseño - Transición - Operación - Mejora Continua	Sistema de Valor del Servicio (SVS): - Principios rectores - Gobierno - Cadena de valor - Prácticas - Mejora continua
Unidad de gestión	10 procesos principales	26 procesos y 4 funciones	34 prácticas de gestión (General, Servicio, Técnica)
Concepto de valor	Entrega de valor (unidireccional: proveedor a cliente)	Creación de valor a través del ciclo de vida	Co-creación de valor (colaborativa: proveedor + consumidor)
Relación con otros marcos	Limitada, enfoque propietario	Integración parcial (ISO 20000)	Integración nativa con Lean, Agile, DevOps
Modelo de operación	Reactivo y basado en estabilidad	Planificado y secuencial	Flexible, iterativo y multimodal

Fuente: Elaboración propia a partir de Axelos (2019) e ITSM.tools (2025)

2.1.3. EL SISTEMA DE VALOR DEL SERVICIO (SVS)

El SVS constituye el elemento central de ITIL 4 y "describe cómo todos los componentes y actividades de la organización trabajan juntos como un sistema para permitir la creación de valor y su propósito es asegurar que la organización cocree valor continuamente con todas las partes interesadas a través del uso y gestión de productos y servicios" (AXELOS, 2019, p. 36).

El modelo opera con dos entradas fundamentales las cuales son la oportunidad y la demanda, que desencadenan actividades dentro del sistema, cuyo resultado final es la generación de valor para la organización, sus clientes y otras partes interesadas.

Los componentes principales del SVS son cinco:

- Los principios guía.
- La gobernanza
- La cadena de valor del servicio
- Las prácticas.
- La mejora continua.

La arquitectura del SVS "permite específicamente flexibilidad y desalienta el trabajo aislado", de modo que las actividades de la cadena de valor y las prácticas "no forman una estructura fija y rígida, sino que se pueden combinar en múltiples flujos de valor para abordar las necesidades de la organización en una variedad de escenarios" (AXELOS, 2019, pág. 37).

Con estos componentes, el SVS soporta muchos enfoques de trabajo, como Agile, DevOps y Lean, así como la gestión tradicional de procesos y proyectos, con un modelo operativo flexible orientado al valor.



Figura 5: El sistema de valor del servicio ITIL

Fuente: ITIL Base, ITIL 4 Edición

2.1.3.1.LA CADENA DE VALOR DEL SERVICIO

La cadena de valor del servicio es "un modelo operativo que describe las actividades clave necesarias para responder a la demanda y facilitar la realización de valor a través de la creación y gestión de productos y servicios" (AXELOS, 2019, pág. 57). A diferencia de los modelos lineales tradicionales, esta cadena es flexible y permite crear múltiples flujos de valor combinando sus seis actividades principales:

- Planificar
- Mejorar
- Participar
- Diseño y Transición
- Obtener/Construir
- Entregar y dar Soporte.

Desde esta perspectiva, la práctica de Gestión de Incidencias debe entenderse como un mecanismo que activa y coordina actividades de la cadena de valor, más que como un conjunto de pasos operativos. Por ejemplo:

- **Participar (engage):** La comunicación con usuarios y áreas afectadas no es accesorio, sino

un componente crítico para alinear expectativas, confirmar restauración y mantener confianza. Si no existe ticket formal, la comunicación queda fragmentada y el usuario no tiene visibilidad del estado del incidente.

- **Entrega y soporte (deliver and support):** Aquí ocurre el restablecimiento operativo. Sin embargo, si el evento no se registra formalmente, se pierde la evidencia necesaria para medir tiempos de respuesta y resolución, y por tanto se imposibilita controlar el desempeño.
- **Mejorar (improve):** ITIL 4 considera la mejora como actividad permanente. Sin datos consistentes de incidentes (frecuencia, impacto, reincidencia), la mejora se vuelve intuitiva y reactiva, debilitando la gobernanza del servicio.
- **Obtener/construir (obtain/build) y diseño y transición (design & transition):** Estas actividades son clave en incidencias de software, porque muchas resoluciones requieren cambios en aplicaciones o despliegues. La ausencia de trazabilidad impide diferenciar con claridad cuándo un incidente derivó en un cambio, qué versión se liberó, y si la corrección eliminó o no la causa.

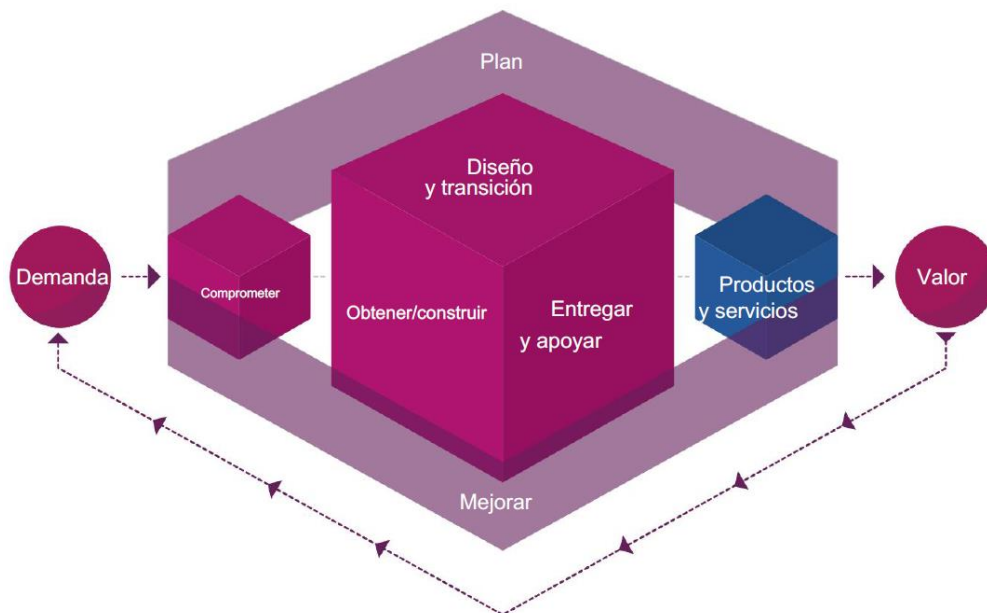


Figura 6: Cadena de valor del servicio ITIL

Fuente: ITIL Base, ITIL 4 Edición

La utilidad de la cadena de valor no radica solo en describir actividades genéricas, sino

en explicar por qué la gestión informal de incidencias de software en Banco Ficensa genera pérdida de control y de valor. Cuando la atención de incidencias se ejecuta por canales dispersos (correos, llamadas, mensajes), se rompe la lógica de cadena y la organización no logra integrar de forma trazable lo que ocurre en “entrega y soporte” con lo que debería retroalimentar a “mejorar”, ni conecta el incidente con “diseño y transición” o “obtener/construir” para prevenir recurrencias. En términos prácticos, el incidente se atiende como un evento aislado y no como un insumo para mejorar el servicio.

2.1.3.2. ENFOQUE HOLÍSTICO: LAS CUATRO DIMENSIONES

El SVS se apoya en el principio de que la gestión de servicios no puede evaluarse únicamente desde procesos. Por ello, ITIL 4 establece cuatro dimensiones que deben considerarse de forma balanceada para lograr servicios efectivos. Estas dimensiones son: organizaciones y personas; información y tecnología; socios y proveedores; flujos de valor y procesos (AXELOS, 2019).

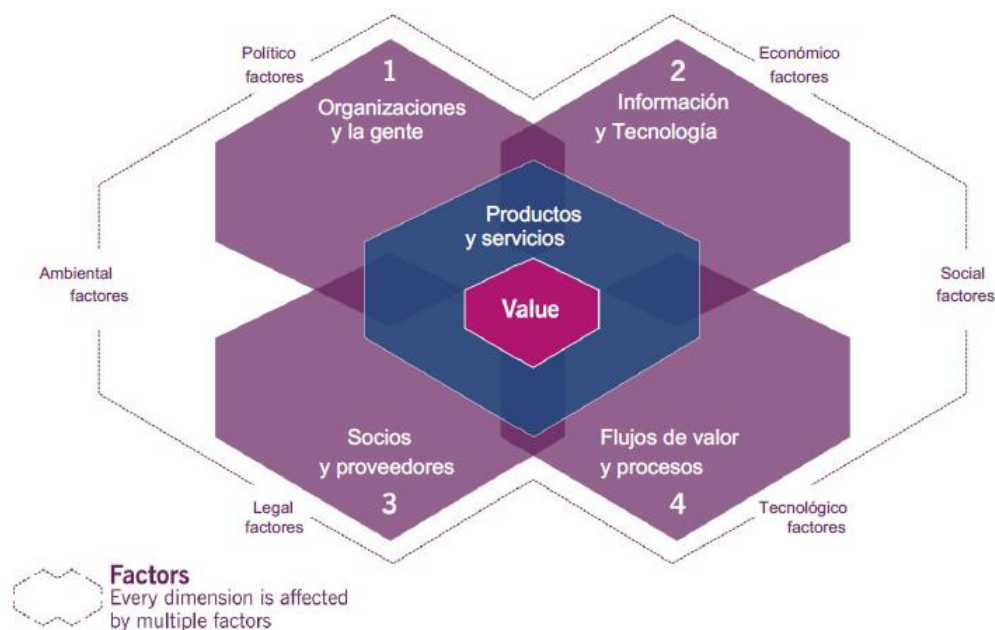


Figura 7: Las cuatro dimensiones de la gestión de servicios

Fuente: ITIL Base, ITIL 4 Edición

AXELOS (2019) advierte que las cuatro dimensiones representan un enfoque holístico y que no mantener equilibrio puede conducir a servicios subóptimos (p. 34). Esta afirmación es especialmente relevante para el problema estudiado, ya que la brecha de Banco Ficensa

(incidencias de software fuera del esquema formal) no se explica solo por ausencia de “un procedimiento”, sino por una desalineación entre dimensiones.

1. **Organizaciones y personas:** En la gestión informal, el rol del usuario, del área de desarrollo y del soporte tiende a mezclarse ya que no se define con precisión quién recibe, quién clasifica, quién prioriza y quién autoriza escalamiento. Desde ITIL 4, esto afecta directamente la capacidad de actuar con consistencia. Una práctica formal requiere roles claros (por ejemplo, mesa de servicio como punto de contacto, soporte aplicativo, desarrollo, y responsables de negocio), porque el desempeño no puede medirse si la responsabilidad operativa es difusa.
2. **Información y tecnología:** ITIL 4 no entiende tecnología solo como herramienta, sino como parte del sistema que habilita trazabilidad y aprendizaje. Si un incidente no se registra, la organización pierde información crítica como ser historial, patrones, tiempos, vínculos con cambios o problemas. En banca, esta pérdida es grave porque limita el control del riesgo operacional asociado a fallas recurrentes en aplicaciones críticas. Así, la herramienta de tickets no es “un requisito administrativo”, sino la base para medición y mejora.
3. **Socios y proveedores:** Las incidencias de software suelen implicar dependencias de proveedores de plataformas, integraciones, o terceros que soportan módulos específicos. Si la gestión es informal, no hay evidencia estructurada de tiempos de atención de terceros, ni de causas asociadas a componentes externos. Esto complica la gestión contractual y la rendición de cuentas, afectando niveles de servicio.
4. **Flujos de valor y procesos:** La ausencia de un flujo formal implica que cada incidencia inicia y finaliza en canales distintos, sin reglas consistentes de categorización, prioridad, escalamiento o cierre. ITIL 4 enfatiza flujos de valor configurables.

En síntesis, las cuatro dimensiones nos permiten visualizar la problemática identificada como una brecha sistémica: la gestión informal falla porque no integra personas, información, proveedores y flujos bajo una misma estructura.

Si bien ITIL 4 comprende un Sistema de Valor del Servicio integral con sus cuatro dimensiones, principios guía y treinta y cuatro prácticas de gestión, el presente trabajo no adopta

el marco en su totalidad. El estudio se circunscribe específicamente a la práctica de Gestión de Incidencias (*Incident Management*), de la cual retoma sus principios de registro, clasificación, priorización, escalamiento y cierre. Las prácticas de Gestión de Problemas, Gestión de Cambios y Gestión de Niveles de Servicio se reconocen como líneas de continuidad futura y quedan fuera del alcance del diseño propuesto (AXELOS, 2019).

2.1.3.3.MEJORA CONTINUA Y CO-CREACIÓN DE VALOR

ITIL 4 establece que la mejora continua ocurre en toda la organización y en todos los niveles, desde el estratégico hasta el operativo (AXELOS, 2019). Asimismo, proporciona un modelo estructurado de mejora continua que refuerza el vínculo entre iniciativas de ITSM y la visión organizacional (AXELOS, 2019). En el plano de incidencias, esta idea se traduce en un punto crítico: sin datos no hay mejora.

En Banco Ficensa, el problema actual incluye ausencia de registro centralizado, falta de medición sistemática de tiempos y reincidencia, y asignación informal al área de desarrollo. Bajo el enfoque de mejora continua, estos elementos constituyen barreras directas para:

- Identificar qué sistemas generan más incidencias y con qué frecuencia.
- Determinar si los tiempos de respuesta y resolución son adecuados.
- Medir reincidencias que podrían señalar problemas subyacentes.
- Priorizar mejoras basadas en evidencia, y no en percepción.

La co-creación de valor, por su parte, implica que el valor surge de la interacción entre proveedor de servicios y partes interesadas (AXELOS, 2019). En banca, esta interacción es especialmente sensible: cuando una aplicación crítica falla, el “valor” no es simplemente restaurar un servidor, sino recuperar la capacidad operativa que sostiene atención, transacciones, cumplimiento y continuidad. Por tanto, la gestión de incidencias debe diseñarse no solo para resolver técnicamente, sino para restaurar valor percibido por el negocio, minimizando impacto y protegiendo confianza.



Figura 8: El modelo de mejora continua

Fuente: ITIL Base, ITIL 4 Edición

2.1.4. GESTIÓN DE INCIDENCIAS EN ITIL 4

Un incidente se define formalmente en ITIL 4 como una interrupción no planificada de un servicio o una reducción en la calidad de un servicio (AXELOS, 2019, pág. 121).

Un incidente se define formalmente en el ámbito de la gestión de servicios como cualquier interrupción no planificada de un sistema o una reducción en la calidad de su prestación, evento que requiere ser registrado y gestionado para garantizar su resolución en un margen de tiempo que satisfaga las expectativas organizacionales (Gunawana y otros, 2024). Para asegurar que dichas expectativas sean realistas, la literatura establece que los tiempos objetivo de resolución deben estandarizarse mediante Acuerdos de Nivel de Servicio (SLA) (Girsang y otros, 2018).

Asimismo, los incidentes deben priorizarse según una clasificación estructurada con el fin de asegurar que aquellos eventos que generan un mayor impacto crítico en el negocio sean atendidos con inmediatez (Girsang y otros, 2018).

En organizaciones con un alto grado de dependencia tecnológica, la ausencia de un proceso estructurado para atender estas interrupciones puede derivar en efectos en cascada que vulneren la continuidad del negocio y la estabilidad operativa de la empresa. Estudios recientes

subrayan que la capacidad de gestionar incidentes de forma sistémica, integrando marcos de trabajo como ITIL, es un componente central para mantener la resiliencia operativa y alcanzar la alineación estratégica entre las necesidades del negocio y el departamento de TI (Dzemydienė y otros, 2024).

En paralelo, normativas internacionales requieren que las organizaciones establezcan procesos documentados para definir responsabilidades, categorizar eventos y registrar de manera sistemática la información necesaria para evaluar el desempeño, lo que permite la mejora continua del sistema de gestión de servicios.

2.1.4.1.FLUJO OPERATIVO

Aunque las versiones recientes de ITIL promueven la flexibilidad, la literatura especializada en sistemas de información identifica un algoritmo de resolución estructurado y común en la gestión de incidentes (Dzemydienė y otros, 2024). Este ciclo operativo comprende:

- Identificación y registro del incidente: Todo incidente debe documentarse formalmente en un sistema ITSM.
- Clasificación y categorización: Permite agrupar incidentes por tipo de servicio afectado y facilitar análisis posteriores.
- Priorización: Se determina combinando impacto y urgencia. En el sector bancario, la indisponibilidad de un sistema transaccional crítico requiere prioridad inmediata frente a incidencias de bajo impacto administrativo.
- Diagnóstico inicial y resolución en primera línea: La mesa de servicio actúa como punto único de contacto (SPOC).
- Escalamiento funcional: Si no se resuelve en primera línea, se transfiere al equipo especializado correspondiente.
- Restauración del servicio y cierre formal: Incluye validación con el usuario afectado.

ManageEngine (2024) destaca que la automatización dentro de plataformas ITSM modernas permite configurar reglas de asignación automática, gestión de SLA y generación de reportes en tiempo real, lo cual reduce los tiempos de resolución y mejora la trazabilidad. En el caso de Banco Ficensa, donde ya se dispone de ServiceDesk Plus, la integración formal de las incidencias de software dentro de este flujo representa una oportunidad metodológica concreta

para cerrar la brecha identificada.

2.1.4.2.ROLES EN LA GESTIÓN DE INCIDENTES

La asignación de roles bajo marcos de gestión como ITIL trasciende la descripción tradicional de puestos jerárquicos; implica la definición de responsabilidades puntuales sobre el resultado final del servicio. En el contexto de la atención de incidencias, las investigaciones empíricas sobre madurez de procesos identifican funciones fundamentales que deben operar de manera coordinada para evitar la formación de cuellos de botella (Gunawana y otros, 2024).

- **Gestor de Incidentes (Incident Manager):** Actúa como el propietario del proceso. Su responsabilidad no es técnica, sino de gobernanza ya que asegura que el flujo operativo se cumpla, monitorea los tiempos de respuesta (SLA) y lidera la comunicación en situaciones de crisis.
- **Agente de Mesa de Servicio (Service Desk Agent):** Es la primera línea de defensa y la cara visible de TI ante el usuario. Su rol exige habilidades híbridas como ser las técnicas para el diagnóstico inicial y blandas para la gestión de la ansiedad del usuario afectado.
- **Soporte Técnico Especializado (Niveles 2 y 3):** Expertos en dominios específicos (desarrollo, bases de datos, redes) que intervienen cuando la incidencia supera la capacidad del primer nivel. Su participación debe ser quirúrgica y gestionada para evitar que se conviertan en cuellos de botella.

Es importante notar que, en organizaciones modernas, estos roles pueden asignarse dinámicamente. Por ejemplo, ante una incidencia crítica de seguridad, un especialista en ciberseguridad podría asumir temporalmente la coordinación, demostrando la flexibilidad que ITIL 4 promueve frente a estructuras estáticas.

2.1.4.3.DIFERENCIAS ENTRE INCIDENTE, PROBLEMA Y CAMBIO

La ambigüedad conceptual entre estas tres dimensiones es catalogada en la literatura académica como una de las causas primarias de ineficiencia y recurrencia de fallas en las unidades de TI (Girsang y otros, 2018). Para Banco Ficensa, distinguir con rigurosidad cada práctica es un requisito ineludible en el camino hacia la madurez de su gobernanza de servicios. A continuación, se define cada concepto y su respectiva interrelación:

- **Gestión de Incidentes:** Tiene como propósito restaurar la operación normal del

servicio con la mayor rapidez posible, minimizando el impacto negativo sobre los usuarios y los procesos del negocio. Su orientación principal es operativa y de corto plazo, debido a que atiende interrupciones o degradaciones del servicio que afectan la continuidad de la actividad institucional.

- **Gestión de Problemas:** Se enfoca en identificar, analizar y gestionar las causas reales o potenciales de uno o más incidentes. Su finalidad no es únicamente resolver una interrupción puntual, sino reducir la probabilidad y el impacto de incidentes futuros mediante el análisis de causa raíz, la documentación de errores conocidos y la definición de soluciones temporales o definitivas.
- **Control de Cambios:** Tiene como propósito maximizar la cantidad de cambios exitosos en servicios, productos o componentes tecnológicos, asegurando que los riesgos hayan sido evaluados, que exista una autorización adecuada y que el cronograma de cambios sea gestionado de forma ordenada. Esta práctica no aplica únicamente a los cambios derivados de la gestión de problemas, sino a todo cambio que pueda afectar directa o indirectamente los servicios, incluyendo modificaciones en infraestructura de TI, aplicaciones, documentación, procesos, relaciones con proveedores u otros componentes del entorno tecnológico. En este sentido, no debe entenderse únicamente como una práctica de control del riesgo, sino como un mecanismo orientado a equilibrar la eficacia del cambio, la capacidad de procesamiento (throughput), el cumplimiento de los procedimientos de autorización y el control de riesgos.

Tabla 2: Comparación conceptual entre incidente, problema y cambio

Concepto	Propósito	Enfoque temporal	Relación con SLA	Criterio Principal de Gestión
Incidente	Restaurar servicio rápidamente	Corto plazo	Directa	Rapidez de restauración y continuidad del servicio
Problema	Identificar y eliminar causa raíz	Mediano-largo plazo	Indirecta	Análisis de causa raíz, prevención y aprendizaje
Cambio	Implementar modificaciones autorizadas y controladas	Variable	Puede afectar SLA	Equilibrio entre eficacia, capacidad de procesamiento, cumplimiento y control de riesgos

Fuente: Elaboración Propia

ManageEngine (2025) ilustra esta relación como un ciclo virtuoso: el incidente dispara la

acción inmediata, el problema aporta el entendimiento profundo, y el cambio ejecuta la mejora definitiva. Sin esta distinción, la organización corre el riesgo de caer en un ciclo perpetuo de atender las mismas situaciones de manera cíclica sin lograr nunca la estabilidad operativa (problemas y cambios).

2.1.5. LA MESA DE SERVICIO COMO FUNCIÓN ESTRATÉGICA

Banco Ficensa ya dispone de una Mesa de Servicio apoyada en una plataforma tecnológica para el registro y seguimiento de diferentes solicitudes de TI. Por esta razón, la presente propuesta no contempla la adquisición o implementación de una nueva herramienta, sino la integración de las incidencias de software de las áreas de Negocios y Operaciones dentro del esquema existente. Para ello, se plantea definir un flujo formal alineado con ITIL 4 que permita registrar, clasificar, priorizar, asignar, escalar, dar seguimiento y cerrar cada caso de manera trazable.

Desde una perspectiva académica, la Mesa de Servicio se concibe como un componente crítico del sistema de gestión de servicios, ya que articula personas, procesos y tecnología para garantizar la continuidad operativa y la calidad percibida del servicio (Stuart D. Galup, 2009). En este sentido, no es simplemente una unidad técnica, sino una función organizacional que influye directamente en la experiencia del usuario y en la percepción del desempeño del área de TI.

En el contexto de esta investigación, la Mesa de Servicio adquiere especial relevancia debido a que el problema identificado no radica en la inexistencia de una herramienta tecnológica, sino en la ausencia de un esquema formal y estandarizado para gestionar incidencias de software. Por tanto, la Mesa de Servicio representa el punto de entrada natural para estructurar el ciclo de vida de las incidencias, asegurar su trazabilidad y generar datos medibles que respalden la toma de decisiones estratégicas.

2.1.5.1.DIFERENCIA ENTRE SERVICE DESK Y HELP DESK

Aunque los términos Service Desk (Mesa de Servicio) y Help Desk (Mesa de Ayuda) suelen emplearse de manera intercambiable en el ámbito tecnológico, la literatura académica sobre Gestión de Servicios de TI (ITSM) establece diferencias conceptuales y operativas sustanciales que reflejan el nivel de madurez de la organización (Tang & Todo, 2013).

El Help Desk tradicional se concibe como una función de naturaleza eminentemente

táctica y reactiva, cuyo objetivo primordial es la reparación inmediata de fallos informáticos bajo un modelo de ruptura y reparación (break-fix). Las investigaciones en sistemas de información señalan que su alcance operativo suele limitarse a proveer soporte técnico de primer nivel para la resolución expedita de incidentes puntuales, operando como un silo que rara vez se integra con las metas estratégicas del negocio (Petersen, 2019).

En contraste, la Mesa de Servicio se erige como un componente estratégico y holístico. De acuerdo con estudios empíricos sobre la implementación de ITSM, un Service Desk maduro trasciende la simple corrección de errores; actúa como el Punto Único de Contacto (SPOC) que no solo atiende incidentes, sino que gestiona integralmente el catálogo de servicios, coordina escalamientos complejos, administra los Acuerdos de Nivel de Servicio (SLA) y asume un rol proactivo en la prevención de fallas mediante la alimentación continua de bases de conocimiento (Tang & Todo, 2013).

Mientras que un Help Desk aislado concentra sus esfuerzos de manera transaccional en cerrar tickets individuales, una Mesa de Servicio estructurada bajo normativas globales (como ITIL) integra la atención de incidencias en un ecosistema que evalúa constantemente el impacto financiero y operativo sobre el negocio (Virda Alfadina y otros, 2025). Para Banco Ficensa, asimilar esta distinción resulta crucial, ya que representa la transición necesaria de una cultura de soporte puramente reactiva hacia un modelo de gobernanza orientado a la mejora continua y la creación de valor.

2.1.5.2.RELACIÓN CON LA CADENA DE VALOR DEL SERVICIO.

Dentro del Sistema de Valor del Servicio (SVS) de ITIL 4, la Mesa de Servicio se vincula principalmente con la actividad “Participar” y “Entrega y Soporte” de la cadena de valor del servicio. Esta relación debe comprenderse al mismo nivel de relevancia, debido a que la Mesa de Servicio no solo coordina la atención de incidentes y solicitudes, sino que también constituye el principal canal de interacción táctica y operativa con los usuarios. En consecuencia, su función no se limita a la resolución técnica de eventos, sino que también permite capturar necesidades, expectativas, percepciones, retroalimentación y requerimientos de las partes interesadas.

Sin embargo, su impacto no se limita a estas dos actividades. La información recopilada por la Mesa de Servicio también alimenta otras actividades de la cadena de valor, entre ellas:

- La actividad de “Mejorar”, mediante el análisis de tendencias, métricas, reincidencias, retroalimentación de usuarios y oportunidades de mejora.
- La actividad de “Participar”, al proporcionar información útil sobre servicios nuevos o modificados, necesidades de soporte, comunicación con usuarios y soporte temprano.
- La actividad de “Planificar”, cuando la información operativa permite identificar componentes, recursos o capacidades requeridas para resolver incidentes o atender solicitudes de servicio.

La propuesta de formalización de la gestión de incidencias depende directamente de la capacidad de la Mesa de Servicio para capturar información estructurada, clasificar correctamente los eventos y permitir su análisis posterior. Sin este mecanismo, no es posible implementar indicadores como MTTR (Tiempo Medio de Reparación o Recuperación), tasa de reincidencia o cumplimiento de SLA, que constituyen parte central de los objetivos específicos de este estudio.

2.1.5.3.PLATAFORMAS ITSM: EL CASO DE MANAGE ENGINE

Las plataformas ITSM representan la materialización tecnológica de los principios y prácticas definidos en marcos como ITIL. Estas herramientas permiten automatizar flujos de trabajo, establecer reglas de priorización, gestionar acuerdos de nivel de servicio y mantener bases de conocimiento integradas (ManageEngine, 2024).

ServiceDesk Plus, de ManageEngine, es una plataforma ITSM que incorpora módulos de gestión de incidentes, problemas, cambios y activos, alineados con buenas prácticas de ITIL. La herramienta permite:

- Configuración de SLA con métricas de respuesta y resolución.
- Automatización de asignación y escalamiento.
- Integración con base de datos de configuración (CMDB).
- Generación de reportes analíticos.

Desde una perspectiva de investigación aplicada, la existencia de esta herramienta en el banco no garantiza por sí misma una gestión eficaz de incidencias. Tal como establece el modelo de referencia de estándares ITSM, la tecnología debe estar acompañada de procesos definidos,

roles claros y métricas alineadas con objetivos organizacionales (IBM, 2006).

En consecuencia, la propuesta de este estudio no se orienta a introducir una nueva herramienta, sino a estructurar metodológicamente el uso de la Mesa de Servicio existente para que funcione como eje estratégico de la gestión de incidencias de software. Esto implica definir criterios de clasificación, priorización, escalamiento y medición coherentes con ITIL 4 y con las exigencias regulatorias del sector bancario.

2.1.5.4.MÉTRICAS E INDICADORES DE DESEMPEÑO (KPIS) EN GESTIÓN DE INCIDENCIAS

La gestión de incidencias no puede considerarse madura si no dispone de un sistema formal de medición. En el marco de ITIL 4, toda práctica debe evaluarse en términos de creación de valor, desempeño y mejora continua (AXELOS, 2019). En consecuencia, las métricas y los indicadores clave de desempeño (KPIs) constituyen el mecanismo técnico que permite transformar la gestión de incidencias de una actividad operativa reactiva a un proceso controlado, medible y alineado con los objetivos organizacionales.

Desde la perspectiva normativa, la norma ISO/IEC 20000-1:2018 exige que la organización establezca, implemente y mantenga mecanismos para monitorear, medir, analizar y evaluar el desempeño del sistema de gestión de servicios, incluyendo la gestión de incidentes (Organización Internacional de Normalización, 2018). Esto implica que la medición no es opcional, sino un requisito estructural para asegurar control, trazabilidad y mejora sistemática.

En el contexto del sector bancario la ausencia de métricas objetivas impide evaluar el impacto real de las interrupciones de software sobre la continuidad del negocio. Por tanto, la formalización de KPIs en gestión de incidencias constituye un elemento central de la propuesta metodológica de esta investigación.

2.1.5.4.1. PRINCIPALES KPIS EN GESTIÓN DE INCIDENCIAS

Tiempo Medio De Resolución (MTTR): El Mean Time to Resolution (MTTR) es uno de los indicadores más utilizados en gestión de incidentes. IBM (2023) define el MTTR como el tiempo promedio requerido para restaurar un servicio después de una interrupción. Este indicador mide eficiencia operativa y capacidad de respuesta. Sin embargo, el MTTR no debe interpretarse de forma aislada. Un MTTR bajo puede reflejar rapidez en la restauración, pero no necesariamente resolución definitiva de la causa raíz. Desde la perspectiva de ITIL 4, este indicador debe

analizarse en conjunto con la gestión de problemas para evitar reincidencias.

Cumplimiento De SLA: El cumplimiento de Acuerdos de Nivel de Servicio (Service Level Agreement, SLA) mide el porcentaje de incidencias resueltas dentro del tiempo acordado con el negocio. IBM (2023) establece que un SLA define formalmente las expectativas de desempeño entre proveedor y cliente interno o externo.

Desde un enfoque de gestión, el SLA traduce objetivos técnicos en compromisos de negocio. En un entorno bancario, un incumplimiento sistemático de SLA puede derivar en riesgos operativos, incumplimientos regulatorios o deterioro de la confianza institucional. Por ello, la implementación de métricas de cumplimiento de SLA no solo mejora la disciplina operativa, sino que fortalece la gobernanza de TI y la rendición de cuentas.

Tasa De Reincidencia: La tasa de reincidencia mide el porcentaje de incidentes que se repiten dentro de un período determinado. Según ManageEngine (2024a), un alto índice de recurrencia suele indicar que la organización está resolviendo síntomas en lugar de causas raíz. Este indicador es clave, ya que permite identificar debilidades estructurales en la gestión de software. Una reducción en la reincidencia evidenciaría que la propuesta no solo acelera la respuesta, sino que mejora la calidad de la solución.

Volumen De Incidentes Por Categoría: La clasificación estructurada de incidencias permite generar estadísticas por tipo de fallo, aplicación afectada, unidad organizativa o nivel de impacto. KnowledgeHut (2023) sostiene que el análisis por categorías permite detectar patrones y áreas de riesgo.

En el sector bancario, este indicador puede revelar concentraciones de riesgo tecnológico en aplicaciones críticas, facilitando decisiones preventivas, asignación de recursos y priorización estratégica.

Satisfacción del usuario (CSAT): El Customer Satisfaction Score (CSAT) mide la percepción del usuario respecto al servicio recibido. IBM (2023) explica que el CSAT evalúa la experiencia del cliente mediante encuestas posteriores a la prestación del servicio. Desde la perspectiva ITSM, este indicador conecta desempeño técnico con percepción de valor. Una gestión de incidencias eficiente en términos de tiempo, pero deficiente en comunicación o claridad, puede deteriorar la satisfacción del usuario.

En el banco, el CSAT permitiría evaluar el impacto reputacional interno del proceso de gestión de incidencias, alineando la práctica con el principio rector de ITIL 4 “centrarse en el valor” (AXELOS, 2019).

Tiempo Medio De Respuesta Inicial: Este indicador mide el tiempo transcurrido desde el registro del incidente hasta el primer contacto con el usuario. Según ManageEngine (2024), la rapidez en la respuesta inicial reduce la percepción de abandono y mejora la experiencia del usuario, aun cuando la resolución requiera más tiempo.

En entornos financieros, donde las interrupciones pueden generar ansiedad operativa, este KPI contribuye a mitigar impacto reputacional interno.

2.1.6. INTEGRACIÓN MACROENTORNO

El análisis del macroentorno revela una transición ineludible en la industria tecnológica global: la gestión de TI ha dejado de ser una disciplina puramente técnica centrada en reparar infraestructura, para convertirse en un paradigma estratégico orientado a la provisión de servicios alineados con los objetivos de negocio (Cots, 2011).

La adopción de marcos de trabajo y estándares internacionales, como ITIL 4 e ISO/IEC 20000, demuestra que el mercado exige a las organizaciones estructurar sus operaciones mediante Acuerdos de Nivel de Servicio (SLA), catálogos definidos y portales de atención estandarizados, con el fin de garantizar la calidad, la resiliencia operativa y la trazabilidad de la información (Jäntti & Lindström, 2026).

En este contexto global de estandarización, la brecha operativa identificada en Banco Ficensa adquiere una dimensión crítica. Mientras que el banco ya ha dado pasos importantes hacia la madurez al implementar un sistema formal para su infraestructura tecnológica, la exclusión de las incidencias de software de este esquema corporativo contradice los principios del Sistema de Valor del Servicio (SVS) que rigen el macroentorno actual.

Como señalan Jäntti y Lindström (2024), la atención informal a través de correos electrónicos y llamadas telefónicas produce datos no estructurados, reduce la transparencia y aumenta significativamente la carga de trabajo, situación que coincide exactamente con la problemática descrita en las áreas de Negocios y Operaciones del banco.

Por consiguiente, el macroentorno valida la necesidad imperativa de la propuesta de

investigación ya que Banco Ficensa no requiere adquirir nueva tecnología, sino alinear su práctica de atención de incidencias de software a la tendencia global de gobernanza y co-creación de valor.

Integrar estas incidencias dentro de un flujo estructurado bajo ITIL 4 y soportado por su actual ServiceDesk permitirá al banco cerrar su brecha de gestión, pasando de un modelo de soporte reactivo y fragmentado a uno proactivo, auditable y plenamente capaz de asegurar la continuidad de sus servicios financieros críticos.

2.2. MICROENTORNO

2.2.1. CONTEXTO DEL SISTEMA FINANCIERO HONDUREÑO

El sistema financiero hondureño está conformado por bancos comerciales, cooperativas de ahorro y crédito, instituciones financieras no bancarias y entidades de servicios complementarios. Este sistema opera bajo un esquema de supervisión prudencial cuyo objetivo principal es preservar la estabilidad financiera, proteger al usuario y mitigar riesgos sistémicos.

En los últimos años, la digitalización del sector ha transformado la forma en que se prestan los servicios financieros. La banca en línea, los pagos electrónicos, las transferencias interbancarias y las aplicaciones móviles han incrementado la dependencia tecnológica de las instituciones financieras. Esta evolución no solo modifica el modelo operativo, sino que introduce nuevas exigencias de control interno, monitoreo y gestión de incidentes tecnológicos.

El Banco Central de Honduras (BCH) establece que la vigilancia de los sistemas de pago tiene como finalidad “velar por el buen funcionamiento, seguridad y eficiencia de los sistemas de pagos” (Banco Central de Honduras, 2026). Esta afirmación refleja que la estabilidad operativa de las plataformas tecnológicas es un elemento clave para el sistema financiero nacional.

Desde una perspectiva del entorno, esto significa que cualquier institución financiera en Honduras opera bajo una expectativa permanente de:

- Alta disponibilidad tecnológica
- Gestión adecuada de riesgos operativos
- Respuesta oportuna ante incidentes
- Control y trazabilidad de eventos

2.2.1.1.DIGITALIZACIÓN Y EXIGENCIAS OPERATIVAS

El proceso de modernización del sistema financiero hondureño ha impulsado iniciativas orientadas a fortalecer pagos digitales y mejorar la eficiencia de las transacciones electrónicas. El BCH ha promovido consultas públicas y proyectos para modernizar el sistema de pagos minoristas, lo cual incrementa la presión sobre las instituciones financieras para asegurar infraestructura robusta y procesos formales de control (Banco Central de Honduras, 2023).

A mayor digitalización, mayor exposición al riesgo tecnológico. Esto convierte la regulación en un factor que, indirectamente, obliga a las entidades a formalizar la gestión de incidentes y fortalecer sus capacidades de monitoreo.

Asimismo, la Comisión Nacional de Bancos y Seguros (CNBS) ha destacado la creciente integración entre banca tradicional y Fintech en Honduras, lo cual amplía el ecosistema tecnológico y agrega complejidad operativa (Comisión Nacional de Bancos y Seguros, 2025). La interoperabilidad, integraciones API y dependencia de terceros aumentan la necesidad de gobernanza tecnológica.

2.2.1.2.PRESIÓN DEL ENTORNO REGULATORIO EN LA OPERACIÓN

Es importante entender que la regulación bancaria hondureña genera una cultura de control y supervisión permanente.

Los entes reguladores en las instituciones financieras exigen que:

- Se mantengan evidencia documental de procesos
- Se reporten eventos relevantes
- Gestionen riesgos operacionales
- Implementen controles tecnológicos formales

Estudios internacionales sobre gobierno corporativo y supervisión bancaria señalan que el riesgo operacional, incluyendo el riesgo tecnológico, constituye uno de los componentes más sensibles dentro de sistemas financieros altamente regulados, debido a su impacto potencial en la estabilidad institucional y sistémica (Basel Committee on Banking Supervision, 2011).

En consecuencia, la regulación no solo define obligaciones legales, sino que moldea el comportamiento organizacional y la formalización de procesos internos.

2.2.1.3.IMPLICACIONES PARA LA GESTIÓN DE INCIDENTES

En el contexto hondureño:

- La indisponibilidad de un sistema bancario puede generar impacto reputacional inmediato.
- Los incidentes tecnológicos pueden derivar en reportes regulatorios.
- Las auditorías internas y externas requieren evidencia trazable.

Por tanto, el entorno regulatorio nacional crea un escenario donde la gestión de incidentes no es opcional ni informal, sino estructuralmente necesaria.

A continuación, se presenta un resumen de los actores relacionados al entorno financiero hondureño:

Tabla 3: Actores del entorno financiero hondureño

Actor	Rol	Implicación operativa
BCH	Vigilancia de sistemas de pago	Exige estabilidad y eficiencia
CNBS	Supervisión prudencial	Presión sobre control interno
Bancos	Prestación de servicios	Dependencia tecnológica
Usuarios	Demanda digital	Expectativa de disponibilidad

Fuente: Elaboración propia.

2.2.2. RIESGO TECNOLÓGICO EN EL SISTEMA FINANCIERO NACIONAL

El proceso de digitalización del sistema financiero hondureño ha generado un entorno operativo altamente dependiente de infraestructura tecnológica. La expansión de la banca electrónica, pagos digitales, transferencias interbancarias automatizadas y aplicaciones móviles ha incrementado la exposición institucional a fallas técnicas, interrupciones de servicio y amenazas cibernéticas.

La Comisión Nacional de Bancos y Seguros (CNBS) reconoce que el uso intensivo de tecnologías de información en instituciones supervisadas incrementa la exposición a riesgos operativos vinculados a fallas tecnológicas y eventos externos. En su normativa sobre gestión de riesgos tecnológicos establece que las instituciones deben implementar mecanismos de control para garantizar disponibilidad, integridad y confidencialidad de la información (Comisión Nacional de Bancos y Seguros, 2022).

Un claro ejemplo de este incremento en los riesgos tecnológicos es el crecimiento de los fraudes cibernéticos que afectan al sistema bancario hondureño. Según un reporte del periódico *El*

Heraldo:

“La Comisión sostiene que el riesgo de fraudes cibernéticos se ha incrementado. Cada día las instituciones financieras del país reciben reclamos de sus clientes sobre que los ciberdelincuentes obtienen su información para sustraer fondos de sus cuentas bancarias por medio de transferencias a cuentas de terceros.” (El Heraldó, 2024).

Este fenómeno no solo refleja la mayor exposición a ciberataques, sino también la necesidad de establecer mecanismos de control tecnológico que mitiguen estas amenazas mediante autenticación reforzada, monitoreo en tiempo real y gestión de incidentes clara y oportuna.

2.2.2.1.FRAUDES CIBERNÉTICOS Y AMENAZAS TECNOLÓGICAS

La regulación financiera hondureña ha empezado a exigir mecanismos específicos para enfrentar los riesgos tecnológicos. En muchos casos, estas amenazas se manifiestan como estafas que buscan vulnerar los sistemas de seguridad de los bancos. En el artículo citado se menciona que se han identificado estafas conocidas como “cuentas mula”, las cuales:

“Han dejado pérdidas estimadas en 350 millones de lempiras y representan un desafío creciente para el sector financiero, ya que implican la obtención ilícita de información para sustraer fondos” (El Heraldó, 2024).

Esto demuestra que los riesgos tecnológicos en el sistema financiero hondureño no se limitan a fallas de hardware o software, sino que incluyen ataques que combinan técnicas de ingeniería social con explotación de vulnerabilidades tecnológicas.

A continuación, se detalle una tabla que define los riesgos tecnológicos más comunes en Honduras:

Tabla 4: Principales Tipos de Riesgos Tecnológicos Identificados en Honduras

Riesgo tecnológico	Descripción	Impacto operativo/financiero
Riesgo de ciberseguridad	Posibilidad de afectación a los sistemas, datos o servicios tecnológicos por accesos no autorizados, ataques informáticos, suplantación o robo de información.	Pérdidas económicas, afectación reputacional, reclamos de clientes y exposición de información sensible.
Riesgo de indisponibilidad de servicios tecnológicos	Interrupción parcial o total de sistemas, aplicaciones o plataformas críticas para la operación bancaria.	Suspensión de operaciones, retraso en procesos internos, afectación al servicio al cliente y pérdida de continuidad operativa.

Riesgo tecnológico	Descripción	Impacto operativo/financiero
Riesgo de fallas en aplicaciones de software	Errores, defectos o comportamientos no esperados en sistemas bancarios que afectan procesos de negocio.	Incidencias operativas, reprocesos, errores transaccionales y aumento en los tiempos de atención y resolución.
Riesgo de control de acceso y autenticación	Debilidades en los mecanismos de identificación, autenticación o autorización de usuarios en los sistemas.	Accesos indebidos, riesgo de fraude, pérdida de confianza y posibles incumplimientos de seguridad.
Riesgo de vulnerabilidades tecnológicas	Existencia de debilidades técnicas en aplicaciones, infraestructura o configuraciones que pueden ser explotadas o generar fallas operativas.	Exposición a ataques, interrupción de servicios críticos, pérdida de integridad de datos y mayores costos de remediación.
Riesgo Tecnológico	Descripción	Impacto Operativo/Financiero
Fraudes Cibernéticos	Robo de credenciales, estafas y transferencias no autorizadas	Pérdidas económicas directas y reclamos de clientes
Phishing y suplantación	Engaños que buscan obtener credenciales	Exposición de información sensible
Fallas de autenticación	Acceso indebido por falta de mecanismos robustos	Riesgo de fraude y pérdida de confianza
Vulnerabilidades en sistemas bancarios	Errores de software o brechas en seguridad	Interrupción de servicios críticos

Fuente: Elaboración propia.

2.2.2.2.DEPENDENCIA DE SISTEMAS CORE Y EXPOSICIÓN A INCIDENTES DE SOFTWARE

El sistema financiero hondureño opera sobre plataformas tecnológicas centrales conocidas como Core bancario, las cuales soportan procesos críticos como apertura de cuentas, procesamiento de créditos, compensaciones, transferencias electrónicas, gestión de tarjetas y conciliaciones contables. Esta alta dependencia tecnológica convierte a cualquier falla de software en un evento con potencial impacto sistémico.

En el contexto nacional, la digitalización acelerada de los servicios financieros ha incrementado la dependencia de aplicaciones móviles, banca en línea y sistemas interconectados. Según la Comisión Nacional de Bancos y Seguros (2022): “Las instituciones supervisadas deben garantizar que los sistemas que soportan procesos críticos del negocio mantengan condiciones de disponibilidad, integridad y confidencialidad” (pág. 6).

Esta exigencia evidencia que los sistemas Core no solo cumplen una función operativa, sino que constituyen la base estructural del funcionamiento financiero institucional.

2.2.3. CONTINUIDAD OPERATIVA EN INSTITUCIONES FINANCIERAS

La continuidad operativa en instituciones financieras constituye un elemento estructural para garantizar la estabilidad, confiabilidad y resiliencia del sistema bancario. En entornos altamente digitalizados, donde la intermediación financiera depende de plataformas tecnológicas, sistemas Core bancarios y canales electrónicos, la interrupción de servicios críticos puede generar impactos operativos, financieros y reputacionales significativos.

Desde una perspectiva normativa internacional, la ISO 22301:2019 define la continuidad del negocio como la capacidad de una organización para continuar la entrega de productos y servicios a niveles aceptables previamente definidos después de una interrupción (Organización Internacional de Normalización, 2019). Esta definición establece que la continuidad no se limita a la recuperación técnica, sino que implica la preservación funcional del servicio bajo condiciones adversas.

En el contexto financiero, esta capacidad se traduce en la obligación de garantizar que los servicios bancarios esenciales como: pagos, transferencias, procesamiento de créditos, consultas de saldo y operaciones electrónicas permanezcan disponibles incluso ante incidentes tecnológicos, fallas de infraestructura o eventos disruptivos.

2.2.3.1. IMPACTO DE INCIDENTES DE SOFTWARE EN LA CONTINUIDAD OPERATIVA BANCARIA

El sistema financiero hondureño opera actualmente sobre plataformas tecnológicas que soportan procesos críticos como transferencias electrónicas, consultas en línea, procesamiento de créditos, compensaciones interbancarias y operaciones de tarjetas. Esta alta dependencia de sistemas informáticos convierte a los incidentes de software en un riesgo operativo relevante.

La Comisión Nacional de Bancos y Seguros (2022). establece que: “Las instituciones supervisadas deberán garantizar la disponibilidad, integridad y confidencialidad de la información y de los sistemas que soportan los procesos críticos del negocio” (pág. 5).

Esto implica que cualquier interrupción derivada de errores de programación, fallas en actualizaciones, defectos en bases de datos o problemas de integración entre aplicaciones puede

afectar directamente la continuidad operativa.

En la siguiente tabla se detallan los tipos de incidentes de software más comunes a nivel bancario en honduras:

Tabla 5: Incidentes de Software y su Impacto en Operaciones Bancarias

Tipo de Incidente de Software	Ejemplo en entorno bancario	Impacto en Continuidad
Error en actualización	Parche defectuoso que bloquea transferencias	Suspensión temporal de servicios electrónicos
Falla en base de datos	Inconsistencia en saldos	Retrasos operativos y reclamos
Caída de sistema Core	Sistema fuera de línea	Paralización de operaciones en sucursales
Error de integración	Fallo entre app móvil y sistema central	Interrupción de transacciones digitales
Saturación de sistema	Lentitud en procesamiento	Degradación del servicio

Fuente: Elaboración propia.

2.2.3.2.EFECTOS OPERATIVOS DE INCIDENTES DE SOFTWARE

Cuando ocurre un incidente crítico de software, la institución puede experimentar:

- Interrupción total del servicio
- Procesamiento manual temporal
- Incremento de reclamos
- Activación de protocolos de contingencia
- Riesgo reputacional

Desde la perspectiva regulatoria, la CNBS (2022) indica que las entidades deben implementar controles que permitan restaurar los servicios tecnológicos en tiempos razonables, lo que evidencia la necesidad de procesos formales de gestión de incidentes.

2.2.3.3.CONTINUIDAD OPERATIVA Y RESTAURACIÓN DE SERVICIOS

En instituciones financieras altamente digitalizadas, la continuidad operativa depende directamente de la capacidad para:

- Detectar rápidamente el incidente
- Clasificar su criticidad
- Escalar técnicamente el problema

- Restaurar el servicio dentro de los límites establecidos
- Documentar y analizar la causa raíz

Los incidentes de software pueden tener efectos sistémicos si afectan aplicaciones Core o servicios interbancarios. Por ello, la gestión estructurada de incidentes se convierte en un mecanismo fundamental para preservar la estabilidad operativa.

Tabla 6: Relación Entre Incidente de Software y Nivel de Impacto Operativo

Nivel de Incidente	Característica	Consecuencia Operativa
Bajo	Error aislado sin afectar transacciones	Corrección interna sin impacto externo
Medio	Fallo parcial en módulo específico	Interrupción limitada de servicios
Alto	Caída de sistema crítico	Suspensión general de operaciones digitales
Crítico	Fallo en sistema Core bancario	Paralización institucional temporal

Fuente: Elaboración propia.

2.2.3.4.APLICACIÓN EN EL CONTEXTO INSTITUCIONAL: BANCO FICENSA

A nivel institucional, el Manual de Proceso Gestión de Tecnologías de Información y Comunicaciones de Banco Ficensa (2020) establece que la Gerencia de TIC debe contar con un Plan de Recuperación de Desastres (DRP) y participar activamente en la elaboración del Plan de Continuidad del Negocio (BCP), asegurando la cobertura integral de los diferentes escenarios de interrupción (Banco Ficensa, 2020).

El manual señala expresamente que las pruebas del DRP deben basarse en el Análisis de Impacto al Negocio (BIA), el cual permite identificar procesos críticos y definir parámetros técnicos como:

- **RTO (Recovery Time Objective):** tiempo máximo aceptable para restaurar el servicio.
- **RPO (Recovery Point Objective):** máxima pérdida de datos tolerable.

Estos indicadores técnicos son fundamentales para la gestión de incidentes de software, ya que establecen límites temporales dentro de los cuales el área de tecnología debe resolver interrupciones críticas.

Asimismo, el manual contempla la implementación de estrategias de redundancia para

sistemas clasificados como críticos (AAA+ y AAA), incluyendo:

- Replicación transaccional hacia centros alternos.
- Monitoreo continuo de disponibilidad.
- Supervisión de integridad de bases de datos.
- Gestión preventiva de bloqueos y cuellos de botella.

Esto evidencia que la continuidad operativa no es un concepto teórico, sino una práctica formalizada y documentada dentro del gobierno tecnológico del banco.

A continuación, se presenta un resumen estructurado de los componentes de continuidad operativa establecidos en el manual institucional:

Tabla 7: Elementos de Continuidad Operativa según Manual de Gestión de Tecnología

Componente	Descripción según el manual	Relación con Gestión de incidentes
Plan de Recuperación de Desastres (DRP)	Documento que establece estrategias de recuperación para los componentes tecnológicos del Banco. Debe actualizarse y probarse anualmente.	Define procedimientos de restauración ante incidentes críticos que afecten disponibilidad de sistemas.
Plan de Continuidad del Negocio (BCP)	Elaborado con participación de TIC para cubrir integralmente escenarios de interrupción.	Garantiza que los servicios financieros críticos continúen operando tras incidentes mayores.
Pruebas Anuales del DRP	Simulaciones de escenarios de desastre con participación de TIC, Seguridad de la Información, Auditoría y áreas de negocio.	Permite validar tiempos reales de respuesta ante incidentes tecnológicos.
BIA (Business Impact Analysis)	Identifica procesos críticos y define prioridades de recuperación.	Determina qué incidentes requieren atención prioritaria y escalamiento inmediato.
RTO (Recovery Time Objective)	Tiempo máximo permitido para restaurar un servicio tras una interrupción.	Establece el límite temporal para resolver incidentes críticos.
RPO (Recovery Point Objective)	Máxima pérdida de datos aceptable en caso de incidente.	Determina tolerancia ante fallos de bases de datos o sistemas transaccionales.
Participación Multidisciplinaria	Incluye Gerente TIC, Oficial de Seguridad, Auditoría y Coordinador de Continuidad.	Asegura gobernanza y control formal en la gestión de incidentes mayores.

Fuente: Banco Ficensa (2017). *Manual de Proceso Gestión de Tecnologías de Información y Comunicaciones* (pág. 10).

2.3.TEORÍAS DE SUSTENTO

2.3.1. TEORÍA DE LA GESTIÓN DE INCIDENCIAS SEGÚN ITIL 4

La Biblioteca de Infraestructura de Tecnologías de Información en su cuarta edición, conocida como ITIL 4, constituye uno de los marcos de referencia más adoptados a nivel mundial para la gestión de servicios de TI. A diferencia de sus versiones anteriores, ITIL 4 incorpora un enfoque sistémico basado en el Sistema de Valor del Servicio (Service Value System, SVS), cuyo propósito es asegurar que todos los componentes y actividades de la organización trabajen de manera integrada para co-crear valor con las partes interesadas (AXELOS, 2019).

Bajo este enfoque, la gestión de incidencias no se limita a la resolución técnica de fallas, sino que se concibe como un mecanismo operativo para restaurar y proteger el valor que los servicios tecnológicos generan para el negocio.

El punto de partida conceptual de esta práctica es la definición misma de incidente: AXELOS (2019) lo precisa como “una interrupción no planificada de un servicio o reducción en la calidad de un servicio” (p. 121). Esta definición, de carácter técnico y operativo, abarca cualquier evento que altere el funcionamiento normal de un servicio, independientemente de su causa, sistema afectado o magnitud, lo que implica la necesidad de contar con mecanismos formales y estandarizados para detectarlo, registrarlo y gestionarlo de manera oportuna.

Respecto al propósito de la práctica, AXELOS (2019) establece que “el propósito de la práctica de gestión de incidentes es minimizar el impacto negativo de los incidentes restableciendo la operación normal del servicio lo más rápido posible” (p. 121). En el sector bancario, donde los sistemas de software sustentan operaciones críticas y continuas, esta relación entre la gestión de incidencias y la continuidad del servicio adquiere una dimensión estratégica vinculada al riesgo operacional y a la estabilidad institucional.

Para que dicho propósito pueda cumplirse, ITIL 4 exige un conjunto mínimo de condiciones operativas. En primer lugar, en cuanto al registro y los tiempos de atención: “cada incidente debe registrarse y gestionarse para garantizar que se resuelva en un tiempo que cumpla con las expectativas del cliente y usuario. Los tiempos de resolución objetivo se acuerdan, documentan y comunican para garantizar que las expectativas sean realistas” (AXELOS, 2019, p. 122).

En segundo lugar, en cuanto a la clasificación y priorización, el marco señala que “los

incidentes se priorizan según una clasificación acordada para garantizar que los incidentes con mayor impacto empresarial se resuelvan primero” (AXELOS, 2019, p. 122).

La ausencia de estas condiciones como ser registro estructurado, tiempos medibles y criterios de priorización en la gestión actual de incidencias de software del área de Negocios y Operaciones de Banco Ficensa configura la brecha central que esta investigación busca caracterizar y corregir.

Desde la perspectiva del Sistema de Valor del Servicio, la gestión de incidencias se integra principalmente en la actividad “Entrega y Soporte” de la cadena de valor, pero también alimenta las actividades de “Participar” y “Mejorar”.

ITIL 4 establece que “los registros de incidentes son un aporte clave para las actividades de mejora” (AXELOS, 2019, p. 123), lo que demuestra que la información histórica generada por los incidentes constituye un insumo estratégico para la optimización del servicio. En consecuencia, la inexistencia de un registro formal no solo afecta la atención inmediata del incidente, sino que debilita la capacidad organizacional de aprendizaje, análisis de tendencias y prevención de recurrencias.

En cuanto a los requerimientos tecnológicos y organizacionales que hacen efectiva la práctica, AXELOS (2019) establece que “la información sobre incidentes debe almacenarse en registros de incidentes en una herramienta adecuada” (p. 122), idealmente con vínculos a cambios, problemas y errores conocidos, a fin de agilizar el diagnóstico y la recuperación.

Asimismo, “la gestión eficaz de incidentes a menudo requiere un alto nivel de colaboración dentro y entre los equipos” (AXELOS, 2019, p. 122), incluyendo la mesa de servicio, soporte técnico, soporte de aplicaciones y proveedores tecnológicos. Estas exigencias evidencian que la práctica no depende exclusivamente de la existencia de una herramienta, sino de la articulación formal de procesos, roles y métricas alineadas al negocio.

Finalmente, ITIL 4 concibe la gestión de incidencias como parte de un sistema orientado a la mejora continua y a la generación sostenida de valor. En el marco de esta investigación, la construcción de una base histórica a partir de fuentes documentales del año 2025 entre esas fuentes están los correos electrónicos, bitácoras y reportes internos, responde precisamente al principio de que la mejora debe sustentarse en información estructurada y medible.

La formalización del registro, la definición de indicadores como el Tiempo Medio de Resolución (MTTR), el cumplimiento de SLA y la tasa de reincidencia, así como la incorporación de un flujo estructurado de clasificación, priorización y escalamiento, constituyen aplicaciones directas de los postulados de ITIL 4.

En consecuencia, la teoría de la Gestión de Incidencias en el marco del Sistema de Valor del Servicio de ITIL 4 proporciona el fundamento conceptual que sustenta la propuesta metodológica de este estudio, al vincular la restauración operativa del servicio con la creación de valor organizacional, la reducción del riesgo tecnológico y el fortalecimiento de la gobernanza de TI en Banco Ficensa.

2.3.2. TEORÍA DEL GOBIERNO CORPORATIVO DE TI

El gobierno corporativo se define como el conjunto de normas, principios y procedimientos que regulan la estructura y funcionamiento de los órganos de dirección de una organización, garantizando transparencia, rendición de cuentas y alineación estratégica (Deloitte, 2016). Su finalidad principal es establecer mecanismos de supervisión que aseguren que las decisiones organizacionales estén orientadas al cumplimiento de los objetivos institucionales y a la adecuada gestión de riesgos.

Downie y O'Brien (2026) , en una publicación oficial de IBM, definen la gobernanza de TI como el conjunto de marcos y estructuras que permiten a las organizaciones optimizar el uso de la tecnología para alcanzar los objetivos empresariales, asegurando control y generación de valor (párr. 1).

En el contexto actual, caracterizado por una alta dependencia tecnológica, este concepto evoluciona hacia el Gobierno Corporativo de Tecnologías de Información (TI), el cual integra la dirección estratégica del negocio con la administración formal de los recursos tecnológicos. Bajo esta concepción, la tecnología deja de ser un elemento exclusivamente operativo y pasa a formar parte del sistema integral de gobierno organizacional.

En la misma línea, Microsoft (2023) sostiene que el gobierno de TI implica establecer políticas, roles y procesos que permitan supervisar el desempeño tecnológico, gestionar riesgos y asegurar cumplimiento normativo dentro de la organización. Desde esta perspectiva, la tecnología no opera de manera aislada, sino bajo mecanismos formales de dirección y control definidos por

la alta administración.

Desde una perspectiva teórica, el Gobierno Corporativo de TI se sustenta en la necesidad de reducir asimetrías de información entre la alta dirección y las áreas operativas, estableciendo estructuras de control que permitan supervisar el uso de los recursos tecnológicos, medir su desempeño y mitigar riesgos asociados. En este sentido, la teoría plantea que las decisiones relacionadas con TI deben integrarse al sistema general de gobierno corporativo, garantizando que:

- Las inversiones en tecnología estén alineadas con los objetivos estratégicos institucionales.
- Los riesgos tecnológicos sean identificados, evaluados y mitigados oportunamente.
- Existan mecanismos de medición del desempeño y control interno.
- Se asegure cumplimiento regulatorio.
- Se genere valor organizacional sostenible.

La formalización práctica de esta teoría se encuentra en marcos internacionales como COBIT 2019, desarrollado por ISACA, el cual establece que el gobierno de la información y la tecnología empresarial tiene como propósito evaluar, dirigir y monitorear el uso de TI para asegurar el logro de los objetivos organizacionales y la adecuada gestión del riesgo (ISACA, 2018). COBIT distingue claramente entre gobierno y gestión, señalando que el gobierno define dirección estratégica y supervisión, mientras la gestión ejecuta las actividades necesarias para cumplir dicha dirección.

Dentro de la estructura de COBIT 2019, el dominio “Entregar, Dar Servicio y Soporte” (DSS) incorpora prácticas específicas relacionadas con la gestión de incidentes tecnológicos, particularmente el objetivo DSS02, el cual establece la necesidad de registrar, clasificar, priorizar y resolver incidentes de manera estructurada y trazable (ISACA, 2018). Este enfoque responde directamente al principio de control interno que sustenta el gobierno corporativo.

En el caso de Banco Ficensa, la gestión actual de incidencias de software en las áreas de Negocios y Operaciones se realiza de forma informal, principalmente mediante correos electrónicos y comunicaciones directas, sin registro centralizado ni indicadores formales de seguimiento. Desde la perspectiva del Gobierno Corporativo de TI, esta situación representa una debilidad estructural, ya que limita la capacidad de la alta dirección para:

- Monitorear el desempeño del servicio tecnológico.
- Evaluar la exposición al riesgo operacional.
- Garantizar trazabilidad de eventos críticos.
- Tomar decisiones basadas en información cuantificable.

En consecuencia, la Teoría del Gobierno Corporativo de TI fundamenta la necesidad de establecer procesos formales que integren control, medición y supervisión dentro de la gestión de incidencias de software. Bajo esta perspectiva, la aplicación de prácticas de ITIL 4 no debe entenderse únicamente como una mejora operativa, sino como un mecanismo alineado al sistema de gobierno corporativo tecnológico del banco, fortaleciendo su control interno, su gestión del riesgo y su alineación estratégica institucional.

2.3.3. TEORÍA DE LOS INDICADORES CLAVE DE DESEMPEÑO (KPIS)

La medición del desempeño constituye un elemento esencial dentro de los sistemas modernos de gestión organizacional, al permitir evaluar de manera objetiva el cumplimiento de objetivos estratégicos y la eficacia de los procesos operativos. En este contexto, los Indicadores Clave de Desempeño (Key Performance Indicators, KPIs) se definen como métricas cuantificables que reflejan el grado de logro de factores críticos para el éxito organizacional.

Kaplan y Norton (1992) establecen que las organizaciones deben traducir su estrategia en objetivos medibles mediante indicadores que permitan monitorear resultados y orientar la toma de decisiones. En su modelo del Balanced Scorecard, los autores argumentan que los indicadores financieros tradicionales resultan insuficientes para evaluar el desempeño integral, por lo que deben complementarse con métricas operativas y estratégicas alineadas a la visión institucional. Desde esta perspectiva, los KPIs no constituyen simples métricas aisladas, sino instrumentos que vinculan la ejecución operativa con la creación de valor organizacional (Kaplan & Norton, 1996).

Desde el ámbito académico, Neely, Gregory y Platts (1995) sostienen que un sistema de medición del desempeño debe diseñarse de manera estructurada, definiendo claramente qué se mide, por qué se mide y cómo se utilizará la información generada. Los autores subrayan que los indicadores deben ser relevantes, consistentes y alineados con los objetivos estratégicos, evitando la proliferación de métricas que no aporten valor para la gestión.

Parmenter (2015) diferencia los KPIs de otros tipos de métricas organizacionales al señalar que un indicador es “clave” cuando impacta directamente en el desempeño crítico del negocio y permite la toma de decisiones correctivas en tiempo oportuno. Para que un KPI sea efectivo, debe ser medible, comprensible, accionable y estar alineado con la estrategia institucional.

En el ámbito de la Gestión de Servicios de Tecnologías de Información, la medición del desempeño forma parte integral del Sistema de Valor del Servicio de ITIL 4. AXELOS (2019) establece que la mejora continua requiere la definición de métricas que permitan evaluar la eficacia de las prácticas de gestión, incluyendo la Gestión de Incidencias. Entre los indicadores comúnmente asociados a esta práctica se encuentran el Tiempo Medio de Resolución (Mean Time to Resolution, MTTR), el porcentaje de cumplimiento de Acuerdos de Nivel de Servicio (SLA), el volumen de incidencias por categoría y la tasa de reincidencia.

Desde una perspectiva teórica, los KPIs cumplen tres funciones fundamentales dentro de la gestión organizacional:

- Función de control: Al permitir comparar resultados reales frente a estándares definidos
- Función de aprendizaje: Al facilitar el análisis de tendencias y la identificación de oportunidades de mejora.
- Función estratégica: Al alinear la operación diaria con los objetivos institucionales.

En el contexto de Banco Ficensa, la gestión informal de incidencias de software impide actualmente la construcción de indicadores confiables que permitan evaluar la eficiencia del área de Desarrollo en la atención de eventos que afectan a las áreas de Negocios y Operaciones. La ausencia de métricas formales limita la capacidad de la alta dirección para monitorear tiempos de atención y resolución, identificar reincidencias y evaluar el cumplimiento de niveles de servicio.

Por consiguiente, la teoría de los Indicadores Clave de Desempeño fundamenta la necesidad de diseñar un sistema de medición específico para la gestión de incidencias de software, el cual permita cuantificar frecuencia, tiempos promedio de resolución, proporción de incidencias sin registro formal y otros indicadores relevantes. La incorporación de KPIs alineados a la práctica de Gestión de Incidencias de ITIL 4 fortalece el control interno, contribuye a la mejora continua y

apoya la reducción del riesgo tecnológico en un entorno financiero regulado.

En consecuencia, esta teoría sustenta el enfoque cuantitativo del presente estudio, al proporcionar el marco conceptual que justifica la construcción, análisis e interpretación de los indicadores propuestos como base para el diseño del modelo formal de gestión de incidencias en Banco Ficensa.

2.4.METODOLOGÍAS DESARROLLADAS

2.4.1. ITIL 4 (PRINCIPAL)

ITIL es un conjunto de mejores prácticas y marcos de trabajo utilizados en la gestión de servicios de tecnología de la información (ITSM). Su última versión fue lanzada en el año 2019, dicho estándar es ampliamente adoptado a nivel mundial desde su creación a finales de la década de 1980 en el Reino Unido. ITIL ha experimentado una evolución continua para adaptarse a las cambiantes necesidades del entorno empresarial y tecnológico.

La versión ITIL 4, introduce una visión integrada de la gestión de servicios basada en el Sistema de Valor del Servicio (SVS), el cual articula principios guía, gobernanza, prácticas de gestión y mejora continua. Esta versión amplía el enfoque tradicional basado en procesos hacia una perspectiva orientada al valor, integrando conceptos modernos como Agile, DevOps y gestión de la experiencia del cliente.

2.4.1.1.JUSTIFICACIÓN DE LA ELECCIÓN DE ITIL 4

La selección de ITIL V.4 como marco de referencia principal para el presente trabajo se fundamenta en su reconocimiento global y en la evidencia académica que respalda su efectividad en contextos similares. Quiñónez Ku (2018), en su investigación aplicada al Departamento de Tics de la Pontificia Universidad Católica del Ecuador, concluye que "ITIL sirve para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI" (pág. 91), tras implementar un modelo de gestión de incidentes bajo este marco y obtener mejoras medibles en la calidad del servicio.

De manera similar, Almendarez Rodríguez & Cuellar Varela (2024) en su propuesta de optimización de la Mesa de Servicio de Banco Davivienda Honduras, validan que la implementación de ITIL 4 mejora la eficiencia operativa y la satisfacción del cliente interno, señalando que el marco "es altamente adaptable, lo que significa que la organización puede

personalizar el marco para satisfacer sus necesidades específicas sin sacrificar la coherencia o la calidad en la gestión de servicios de TI (pág. 33). Igualmente, Rodríguez Archaga (2024), emplea ITIL 4 como eje metodológico central, reafirmando que este marco permite estandarizar procesos, establecer KPIs y mejorar la percepción del soporte técnico interno.

Esta convergencia de evidencia en distintos contextos organizacionales y regionales, incluyendo el entorno centroamericano, confirma la pertinencia de ITIL 4 para el presente proyecto.

2.4.1.2.APLICACIÓN ITIL 4

La aplicación de ITIL 4 en el presente estudio se orienta específicamente a fortalecer la gestión de incidencias de software dentro Banco Ficensa, S.A. Su implementación no implica la adopción completa del marco, sino la adaptación de aquellas prácticas que aportan mayor valor al problema identificado.

La aplicación metodológica contempla los siguientes elementos:

- **Identificación y formalización de procesos clave:** ITIL 4 proporciona prácticas claramente definidas como Gestión de Incidentes, Gestión de Problemas, Gestión de Cambios y Gestión de Niveles de Servicio. Estas prácticas serán utilizadas como base estructural para diseñar un flujo formal y documentado de atención de incidencias.
- **Diseño de flujos de trabajo estructurados:** La metodología orienta la construcción de procesos sistemáticos que aseguren el registro, clasificación, priorización, resolución y cierre de incidentes bajo criterios estandarizados.
- **Priorización basada en impacto y urgencia:** ITIL 4 establece directrices para clasificar incidentes de acuerdo con su impacto en el negocio, elemento crítico en el sector financiero donde la interrupción de servicios puede afectar la continuidad operativa y la reputación institucional.
- **Gestión controlada de cambios:** El marco promueve un enfoque estructurado para implementar modificaciones tecnológicas, reduciendo la probabilidad de incidentes recurrentes derivados de cambios no controlados.
- **Medición y mejora continua:** ITIL 4 fomenta el uso de indicadores clave de desempeño (KPIs) para evaluar la eficiencia y eficacia del proceso de gestión de

incidencias, permitiendo la retroalimentación constante y la mejora continua.

- **Alineación con el valor del negocio:** Uno de los principios fundamentales de ITIL 4 es la co-creación de valor. En el contexto bancario, esto implica que la gestión de incidencias debe contribuir a garantizar la continuidad del servicio financiero, el cumplimiento regulatorio y la mitigación del riesgo operativo.
- **Adaptabilidad al contexto organizacional:** ITIL 4 es flexible y permite su personalización sin perder coherencia metodológica, característica esencial para su implementación en un banco sujeto a normativa prudencial y supervisión estatal.

2.4.2. COBIT 2019 (COMPLEMENTARIA)

2.4.2.1. JUSTIFICACIÓN DE LA SELECCIÓN DE COBIT 2019

La creciente dependencia tecnológica del sector financiero exige un enfoque formal de gobierno y gestión de la información y la tecnología (I&T), que garantice alineación estratégica, control de riesgos y cumplimiento normativo. En este contexto, COBIT 2019 fue seleccionado como marco metodológico debido a su enfoque integral de gobierno corporativo de TI.

COBIT 2019 se define como “un marco de referencia para el gobierno y la gestión de la información y la tecnología dirigido a toda la empresa” (ISACA, 2018, pág. 9). A diferencia de otros marcos operativos centrados únicamente en la prestación de servicios, COBIT integra la perspectiva estratégica, el control interno y la gestión de riesgos dentro de un sistema de gobierno empresarial.

Según ISACA (2018) el sistema de gobierno se compone de siete componentes interrelacionados que permiten diseñar, implementar y monitorear la gobernanza y gestión de TI (págs. 11-13).



Figura 9: Componentes del sistema de gobierno

Fuente: COBIT 2019 (ISACA, 2018).

1. **PROCESOS:** Los procesos representan el conjunto estructurado de prácticas y actividades necesarias para alcanzar objetivos de gobierno y gestión. En el ámbito de la gestión de incidentes, los procesos permiten estandarizar el registro, clasificación, priorización y escalamiento, garantizando consistencia, trazabilidad y control en la atención de eventos tecnológicos (ISACA, 2018).
2. **ESTRUCTURAS ORGANIZATIVAS:** Las estructuras organizativas definen los órganos, comités y roles responsables de la toma de decisiones y supervisión. En el contexto bancario, estas estructuras aseguran que los incidentes críticos sean escalados a niveles estratégicos, vinculando la gestión operativa con el gobierno corporativo y la gestión de riesgos (ISACA, 2018).
3. **PRINCIPIOS, POLÍTICAS Y PROCEDIMIENTOS:** Este componente establece el marco normativo interno que orienta la actuación organizacional. Las políticas y procedimientos formales permiten asegurar coherencia, cumplimiento regulatorio y alineación estratégica en la gestión de servicios y manejo de incidentes tecnológicos (ISACA, 2018).
4. **INFORMACIÓN:** La información constituye un recurso esencial para la toma de decisiones. En gestión de incidentes, la disponibilidad de datos confiables, métricas y reportes permite

evaluar tendencias, medir desempeño y fortalecer el control interno dentro del sistema de gobierno (ISACA, 2018).

5. **CULTURA, ÉTICA Y COMPORTAMIENTO:** COBIT reconoce que la cultura organizacional influye significativamente en la efectividad del gobierno. En el manejo de incidentes, una cultura orientada a la transparencia, reporte oportuno y aprendizaje continuo fortalece la resiliencia institucional (ISACA, 2018).
6. **PERSONAS, HABILIDADES Y COMPETENCIAS:** El Sistema de gobierno requiere personal capacitado con habilidades técnicas y gerenciales adecuadas. En banca, la gestión eficaz de incidentes depende de equipos competentes capaces de responder oportunamente ante eventos tecnológicos críticos (ISACA, 2018).
7. **SERVICIOS, INFRAESTRUCTURA Y APLICACIONES:** Este componente comprende los activos tecnológicos que soportan los procesos de negocio. La adecuada gestión de infraestructura y aplicaciones resulta fundamental para prevenir incidentes, garantizar continuidad operativa y asegurar niveles de servicio acordes al sector financiero (ISACA, 2018).

La elección de COBIT 2019 responde a los siguientes criterios:

- Permite integrar la gestión de incidentes dentro del sistema de gobierno corporativo.
- Facilita la alineación con exigencias regulatorias nacionales, como la Resolución No. 025-2022 de la CNBS.
- Incorpora la optimización del riesgo como objetivo explícito del órgano de gobierno (ISACA, 2018).
- Proporciona un modelo estructurado de procesos, dominios y componentes aplicables al entorno bancario.

Asimismo, COBIT distingue claramente entre gobierno y gestión, estableciendo que “el Gobierno asegura que las necesidades y condiciones de las partes interesadas se evalúan para determinar objetivos empresariales equilibrados” mientras que “la Gestión planifica, construye, ejecuta y monitorea actividades alineadas con la dirección establecida por el órgano de gobierno” (ISACA, 2018, pág. 9).

En consecuencia, la aplicación de COBIT 2019 en esta investigación permite analizar la gestión de incidentes no solo como un proceso técnico, sino como un mecanismo de cumplimiento estratégico y regulatorio dentro del sistema financiero hondureño.

Estos componentes estructuran el sistema de gobierno y sirven como base conceptual para comprender la integración entre la gestión operativa de incidentes y el gobierno corporativo. Sin embargo, en la presente investigación se priorizan principalmente los componentes relacionados con procesos, estructuras organizativas y políticas, por su relación directa con la formalización del proceso de gestión de incidentes de software.

2.4.2.2.APLICACIÓN METODOLÓGICA DE COBIT 2019 EN LA INVESTIGACIÓN

En el desarrollo de la presente investigación, COBIT 2019 se emplea como marco de gobierno complementario que permite fortalecer la supervisión y formalización del proceso de gestión de incidentes implementado bajo la metodología ITIL 4.

Su aplicación metodológica tiene como propósito:

1. Evaluar el nivel actual de formalización de la gestión de incidentes dentro de la institución.
2. Identificar brechas entre las prácticas existentes y los objetivos de gobierno establecidos por COBIT 2019.
3. Diseñar un modelo de mejora alineado con estándares internacionales y con la normativa nacional aplicable al sector financiero.
4. Integrar formalmente la gestión de incidentes dentro del esquema de gobierno corporativo y administración integral de riesgos.

COBIT 2019 organiza sus objetivos en cinco dominios principales (ISACA, 2018):

- EDM – EVALUAR, DIRIGIR Y MONITORIZAR
- APO – ALINEAR, PLANIFICAR Y ORGANIZAR
- BAI – CONSTRUIR, ADQUIRIR E IMPLEMENTAR
- DSS – ENTREGAR, SERVICIO Y SOPORTE
- MEA – MONITORIZAR, EVALUAR Y VALORAR

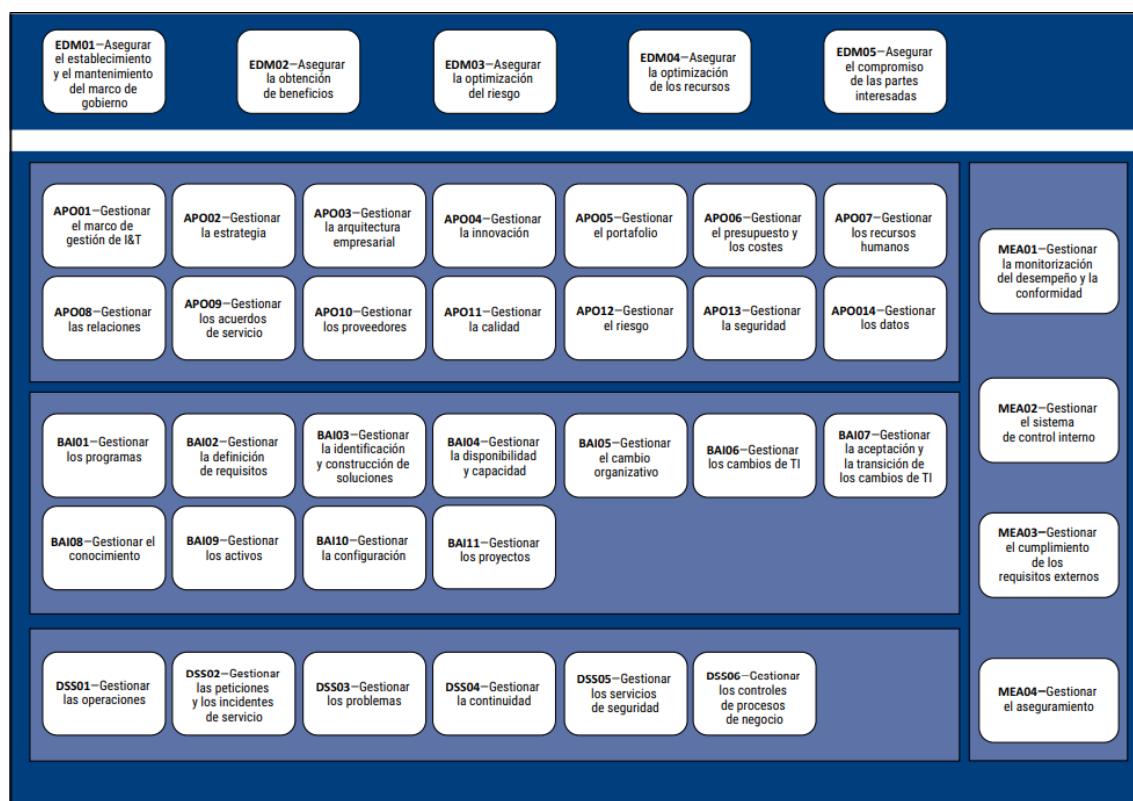


Figura 10: Modelo Core de COBIT

Fuente: COBIT 2019 (ISACA, 2018).

Estos objetivos sirven como marco evaluativo para el diagnóstico institucional y como base para la propuesta de mejora.

2.4.3. INTEGRACIÓN ENTRE ITIL Y COBIT

La combinación de ITIL 4 y COBIT 2019 permite abordar la gestión de incidencias de software desde una perspectiva integral que articula tanto la dimensión operativa como la dimensión de gobierno de las tecnologías de información.

Mientras ITIL 4 proporciona las prácticas y procedimientos necesarios para estructurar el flujo operativo de registro, clasificación, priorización, resolución y cierre de incidentes, COBIT 2019 complementa este enfoque mediante un marco de gobierno que permite asegurar la alineación de dichos procesos con los objetivos estratégicos de la organización, la gestión del riesgo tecnológico y el cumplimiento regulatorio del sector financiero.

En el contexto de esta investigación, ITIL 4 constituye el eje metodológico principal para

el diseño del modelo de gestión de incidencias de software, dado que ofrece directrices específicas para la operación de prácticas como Incident Management, Problem Management y Service Level Management.

Por su parte, COBIT 2019 se emplea como marco complementario de gobernanza, permitiendo contextualizar el proceso dentro del sistema de gobierno corporativo de tecnologías de información y garantizar que la gestión de incidentes contribuya a los objetivos de control, riesgo y cumplimiento establecidos en el entorno bancario.

De esta forma, la integración de ambos marcos permite diseñar una propuesta metodológica que no solo optimiza la gestión operativa de incidencias, sino que también fortalece la supervisión institucional, la trazabilidad de los procesos y la alineación entre la operación tecnológica y las necesidades estratégicas del Banco Ficensa.

Tabla 8: Integración metodológica de ITIL 4 y COBIT 2019

Marco de referencia	Rol metodológico	Alcance dentro de la investigación	Aplicación en el modelo propuesto
ITIL 4	Marco operativo de gestión de servicios	Proporciona prácticas para estructurar la gestión de incidencias de software	Diseño del flujo de registro, clasificación, priorización, escalamiento, resolución y cierre de incidentes
COBIT 2019	Marco de gobierno y control de TI	Permite integrar la gestión de incidencias dentro del sistema de gobierno corporativo	Definición de estructuras organizativas, políticas, control de riesgos y alineación con regulación del sector financiero

Fuente: Elaboración Propia

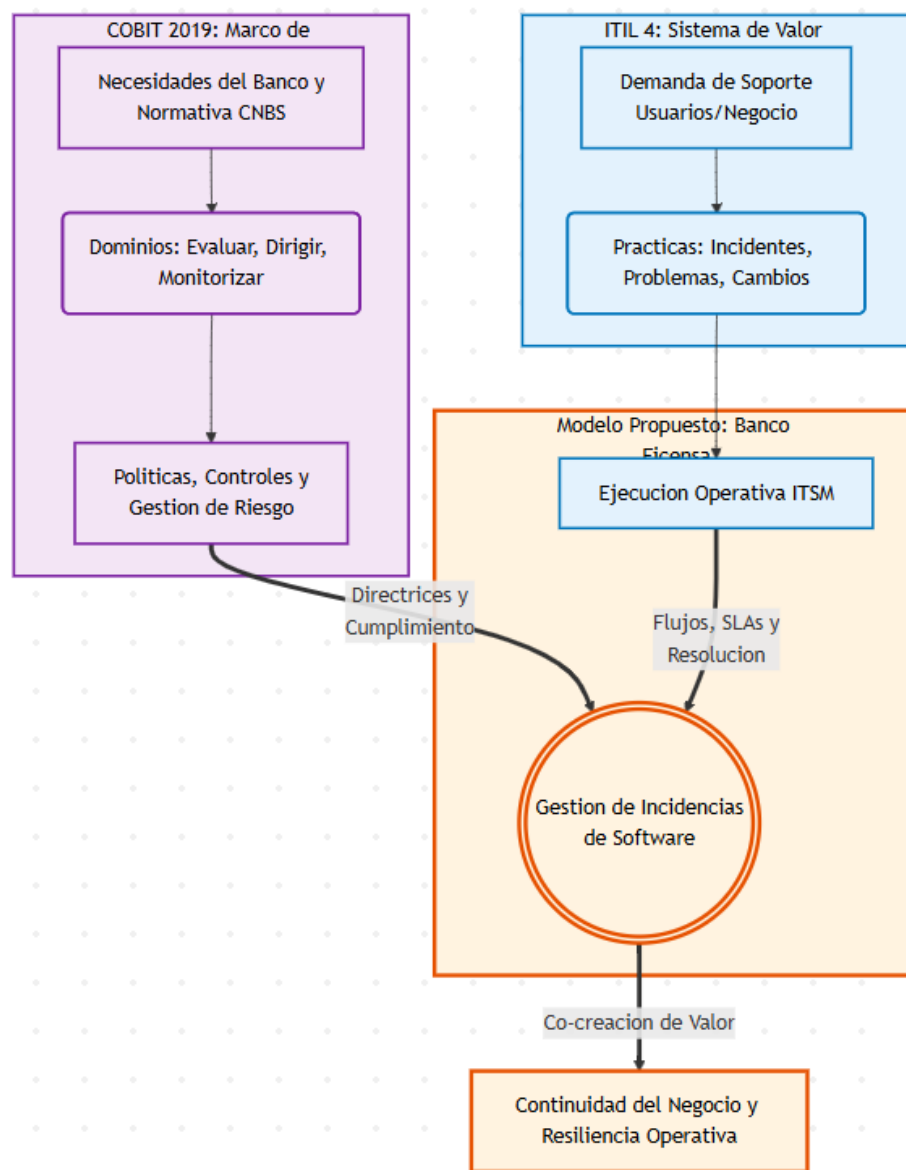


Figura 11: Diagrama integrador de ITIL 4 y COBIT 2019

Fuente: Elaboración Propia.

Es preciso delimitar el alcance metodológico del presente trabajo respecto a los marcos de referencia empleados. La investigación no adopta ITIL 4 de manera integral ni pretende implementar la totalidad de sus prácticas de gestión de servicios; se circunscribe específicamente a la práctica de Gestión de Incidencias (*Incident Management*), de la cual se retoman sus principios de registro, clasificación, priorización, escalamiento y cierre (AXELOS, 2019). Las prácticas de Gestión de Problemas, Gestión de Cambios y Gestión de Niveles de Servicio se reconocen como líneas de continuidad futura y no forman parte del diseño propuesto. De manera complementaria,

COBIT 2019 se emplea como instrumento de gobierno y evaluación de la capacidad del proceso, particularmente a través del objetivo de gestión DSS02, que permite establecer el estado actual (AS-IS) y el estado objetivo (TO-BE) de la capacidad institucional (ISACA, 2018). En consecuencia, ITIL 4 aporta el sustento para el diseño del proceso, mientras que COBIT 2019 aporta el sustento para su medición y gobierno.

2.5. INSTRUMENTOS UTILIZADOS

2.5.1. MANAGE ENGINE SERVICE DESK PLUS.

Para operativizar las prácticas de ITIL 4 definidas en la propuesta, se aprovechará la plataforma institucional existente ManageEngine ServiceDesk Plus, con el propósito de incorporar dentro de su esquema formal las incidencias de software de las áreas de Negocios y Operaciones.



Figura 12: Logo ServiceDesk Plus

Fuente: (Manage Engine, 2026)

ServiceDesk Plus es una solución integral de gestión de servicios que combina la gestión de servicios de TI (ITSM), la gestión de activos de TI (ITAM) y la base de datos de gestión de la configuración (CMDB), integrando además funciones de gestión de servicios empresariales (ESM) para departamentos como recursos humanos, instalaciones y finanzas. Disponible tanto en implementaciones locales (on-premises) como en la nube, ServiceDesk Plus es la opción ideal para las organizaciones que buscan una solución de gestión de servicios empresariales y de TI escalable, segura y ampliable, con un retorno de la inversión garantizado y una alineación nativa con ITIL (ManageEngine, 2025).

ManageEngine (2025) indica que grandes organizaciones a nivel mundial son usuarios activos de la herramienta ServiceDesk Plus. Empresas de renombre internacional como Honda, Disney, Xerox y ABC, entre otras, apoyan la gestión de sus mesas de servicio y soporte técnico operando sobre esta plataforma.

La siguiente figura expone las diferentes versiones de licenciamiento disponibles de

ServiceDesk Plus, las cuales se adaptan a la madurez de los procesos de cada institución.



Figura 13: Versiones De ServiceDesk Plus De Manage Engine

Fuente: (Manage Engine, 2026)

En el marco del presente proyecto, las funcionalidades de ServiceDesk Plus que resultarían más relevantes para la gestión de incidencias son las siguientes:

- **Gestión de Incidentes:** Permite registrar, clasificar, asignar y resolver incidentes bajo un esquema estructurado, asegurando trazabilidad completa y control de tiempos de respuesta.
- **Gestión de Problemas:** Facilita el análisis de causas raíz y la identificación de patrones recurrentes, contribuyendo a la reducción del riesgo tecnológico.
- **Gestión de Cambios:** Establece procedimientos de aprobación y evaluación de impacto para modificaciones en la infraestructura tecnológica, minimizando interrupciones no planificadas.
- **Gestión de Activos y CMDR:** Proporciona una base de datos centralizada que documenta la relación entre activos tecnológicos e incidentes, fortaleciendo la capacidad de diagnóstico.
- **Gestión de SLA y Reportes:** Permite monitorear el cumplimiento de niveles de servicio mediante paneles de control y reportes automatizados, apoyando la medición del desempeño y la mejora continua.

2.5.2. COBIT 2019

Las herramientas temáticas basadas en COBIT 2019 utilizadas en la presente investigación se orientan a proporcionar un marco de referencia para la evaluación de la capacidad del proceso de gestión de incidencias de software, así como para la medición de su desempeño dentro de un enfoque de gobernanza y mejora continua.

2.5.2.1. MATRIZ DE EVALUACIÓN DE CAPACIDAD DEL PROCESO (COBIT 2019)

Como instrumento complementario de diagnóstico se utilizó una Matriz de Evaluación de Capacidad del Proceso basada en COBIT 2019. Su finalidad es determinar el nivel actual de capacidad del proceso de gestión de incidencias de software en las áreas de Negocios y Operaciones de Banco Ficensa, establecer un nivel objetivo y calcular la brecha existente entre ambos estados.

La matriz contempla seis niveles de capacidad: nivel 0, incompleto; nivel 1, ejecutado; nivel 2, gestionado; nivel 3, establecido; nivel 4, predecible; y nivel 5, optimizado. La valoración se realiza mediante el análisis de la evidencia documental disponible, considerando el grado de formalización del proceso, la trazabilidad de los registros, la definición de responsables, la existencia de procedimientos estandarizados, el uso de indicadores y los mecanismos de mejora continua.

Este instrumento se aplica al proceso específico de gestión de incidencias de software analizado en la investigación. Por tanto, su resultado no debe interpretarse como una evaluación general de la madurez de toda la Mesa de Servicio del banco. El formato utilizado se presenta en el anexo. ([Ver Anexo 1](#)).

2.5.2.2. MATRIZ RA DEL PROCESO DE GESTIÓN DE INCIDENCIAS DE SOFTWARE

La matriz RA se establece como un instrumento metodológico clave para la definición y estructuración de roles y responsabilidades dentro del proceso de gestión de incidencias de software en las áreas de Negocios y Operaciones del Banco Ficensa.

Esta herramienta permite asignar de manera clara y formal las responsabilidades asociadas a cada actividad del proceso, diferenciando entre quien ejecuta directamente la actividad y quien rinde cuentas por los resultados obtenidos. De esta forma, se reducen ambigüedades operativas y se asegura una correcta ejecución del flujo de gestión de incidencias, en concordancia

con las buenas prácticas de ITIL 4 y los principios de gobierno de TI promovidos por COBIT 2019.

La matriz se fundamenta en dos tipos de participación:

Responsable (R): quien ejecuta directamente la actividad.

Accountable (A): quien tiene la responsabilidad final y toma decisiones.

En el contexto de esta investigación, la matriz RACI será aplicada al flujo de gestión de incidencias de software, permitiendo:

- Identificar las responsabilidades actuales en la gestión de incidencias (estado actual).
- Detectar vacíos, duplicidades o ambigüedades en la asignación de roles.
- Definir una estructura de responsabilidades propuesta (estado futuro) alineada a ITIL 4.

Este instrumento cumple una doble función metodológica:

- Diagnóstica al evidenciar la gestión informal existente.
- Propositiva al estructurar un modelo organizado, controlado y trazable del proceso.

Su implementación contribuye directamente al fortalecimiento de la gobernanza del proceso, facilitando la rendición de cuentas, el control operativo y la eficiencia en la atención de incidencias de software. ([Ver Anexo 2](#)).

2.5.2.3.INDICADORES CLAVE DE DESEMPEÑO (KPIS)

Como instrumento complementario para la medición del desempeño, se definió una matriz de indicadores clave de desempeño (KPIs) aplicable al proceso de gestión de incidencias de software en las áreas de Negocios y Operaciones de Banco Ficensa. Su propósito es proporcionar una base cuantitativa para evaluar la eficiencia operativa, la trazabilidad de los casos, la reincidencia de las fallas y el nivel de control alcanzado por el proceso.

La selección de los indicadores responde a los objetivos específicos de la investigación y a la necesidad de diferenciar dos momentos de medición. En primer lugar, se establecen indicadores que permiten analizar la situación actual durante el año 2025 a partir de los registros históricos disponibles.

En segundo lugar, se incorporan indicadores de seguimiento que deberán medirse

posteriormente, una vez que las incidencias de software sean integradas formalmente dentro de la Mesa de Servicio institucional y se implemente el flujo propuesto.

Esta diferenciación resulta necesaria debido a que las incidencias de software analizadas no se encontraban incorporadas a un esquema centralizado de registro, clasificación, priorización, seguimiento y cierre. Por consiguiente, la información histórica disponible permite construir una línea base del proceso actual, mientras que la implementación del modelo permitirá generar datos más completos y comparables para evaluar su evolución.

Para establecer la línea base del proceso durante el año 2025, se definieron los siguientes indicadores:

- **Porcentaje de incidencias gestionadas sin registro formal:** Representa la proporción de incidencias atendidas mediante canales no formalizados, como llamadas telefónicas, mensajería instantánea o comunicaciones verbales, respecto al total de casos identificados. Este indicador permite evaluar el nivel actual de formalización y trazabilidad del proceso. Un porcentaje elevado evidencia que una parte significativa de las incidencias se gestiona sin un expediente verificable que permita reconstruir su ciclo de vida.
- **Tiempo promedio de atención:** Corresponde al promedio del tiempo transcurrido entre el reporte inicial de la incidencia y el inicio documentado de su atención. Su medición permite identificar retrasos en la recepción, asignación y primera respuesta del área responsable. Este indicador resulta relevante porque una respuesta tardía puede incrementar el impacto operativo de una falla, aun cuando posteriormente se logre resolver el caso.
- **Tiempo promedio de resolución de incidencias (MTTR, Mean Time to Resolution):** Representa el promedio del tiempo transcurrido entre el reporte inicial de la incidencia y la solución documentada del caso. Para establecer la línea base del año 2025, este indicador se calculará únicamente sobre las incidencias resueltas que cuenten con fecha de reporte y fecha de resolución verificables. El MTTR permite evaluar la eficiencia operativa del proceso e identificar diferencias según área funcional, sistema afectado o nivel de criticidad.
- **Tasa de reincidencia:** Corresponde a la proporción de incidencias que se repiten en el mismo sistema, módulo o proceso respecto al total de casos identificados. Su análisis

permite reconocer fallas recurrentes y determinar si la atención se ha concentrado únicamente en resolver síntomas sin eliminar las causas subyacentes. Una tasa elevada puede evidenciar la necesidad de vincular determinados casos con prácticas complementarias, como la gestión de problemas y el análisis de causa raíz.

Indicadores para el seguimiento futuro del modelo propuesto

- **Cumplimiento de acuerdos de nivel de servicio (SLA):** Representa el porcentaje de incidencias atendidas y resueltas dentro de los tiempos definidos según su nivel de criticidad. Este indicador permitirá evaluar el cumplimiento de los compromisos operativos establecidos con las áreas usuarias y verificar si el proceso responde adecuadamente a las prioridades del negocio. Su medición deberá iniciar una vez que se definan, documenten y comuniquen formalmente los tiempos objetivo-aplicables a las incidencias de software.
- **Porcentaje de incidencias con trazabilidad completa:** Corresponde a la proporción de casos que cuentan con registro formal, clasificación, nivel de prioridad, responsable asignado, evidencia de seguimiento, solución documentada y confirmación de cierre. Este indicador permitirá evaluar si la implementación del modelo corrige la principal brecha identificada en el proceso actual: la ausencia de un historial completo y verificable para cada incidencia.

Los seis indicadores seleccionados permiten evaluar dimensiones complementarias del proceso. El porcentaje de incidencias gestionadas sin registro formal y el porcentaje de casos con trazabilidad completa miden el nivel de formalización y control documental. El tiempo promedio de atención y el MTTR permiten evaluar la oportunidad y eficiencia de la gestión. La tasa de reincidencia facilita la identificación de fallas repetitivas que requieren un tratamiento más profundo. Finalmente, el cumplimiento de SLA permite verificar si el proceso formalizado responde a los compromisos establecidos con el negocio.

La matriz de KPIs se complementa con la matriz de evaluación de capacidad del proceso basada en COBIT 2019 y con la matriz RA. Mientras la primera permite determinar el nivel actual de formalización y la brecha respecto al estado objetivo, la segunda define las responsabilidades asociadas a cada actividad del flujo. La matriz de indicadores permite medir objetivamente los resultados alcanzados por el proceso y evaluar su evolución después de implementar la propuesta.

Los KPIs conforman un sistema integral de instrumentos que permite evaluar, estructurar y mejorar la gestión de incidencias de software en Banco Ficensa. ([Ver Anexo 3](#)).

2.6.CONCEPTUALIZACIÓN

- **Gestión de Servicios de Tecnologías de la Información (ITSM):** La Gestión de Servicios de Tecnologías de la Información (ITSM) es el enfoque organizacional orientado a planificar, diseñar, entregar, operar y mejorar servicios de TI alineados con las necesidades del negocio. ITSM no se centra únicamente en la infraestructura tecnológica, sino en la provisión de valor a través de servicios estructurados y medibles.
- **ITIL:** ITIL es un marco de buenas prácticas para la gestión de servicios de TI que proporciona lineamientos estructurados para la creación, entrega y mejora continua de servicios tecnológicos. En su versión ITIL 4, integra el Sistema de Valor del Servicio (SVS) como modelo central de operación.
- **Sistema de Valor del Servicio (SVS):** El Sistema de Valor del Servicio es el modelo conceptual introducido en ITIL 4 que describe cómo todos los componentes y actividades de una organización trabajan conjuntamente para facilitar la creación de valor a través de los servicios.
- **Incidente:** Un incidente es cualquier interrupción no planificada de un servicio de TI o una reducción en la calidad del mismo. La gestión de incidentes tiene como objetivo restaurar la operación normal del servicio lo antes posible, minimizando el impacto en el negocio.
- **Problema:** Un problema es la causa raíz desconocida de uno o más incidentes. La gestión de problemas busca identificar, analizar y eliminar las causas subyacentes de incidentes recurrentes, reduciendo su probabilidad de repetición.
- **Cambio:** Un cambio es la adición, modificación o eliminación de cualquier elemento que pueda tener impacto en los servicios de TI. La gestión de cambios garantiza que las modificaciones se realicen de manera controlada y con mínimo riesgo operativo.
- **Acuerdo de Nivel de Servicio (SLA):** Un Acuerdo de Nivel de Servicio (SLA) es un compromiso formal entre el proveedor del servicio y el cliente, que define métricas específicas como tiempos de respuesta, tiempos de resolución y niveles de disponibilidad.

- **Indicador Clave de Desempeño (KPI):** Un KPI es una métrica cuantificable utilizada para evaluar la eficacia y eficiencia de un proceso. En la gestión de incidentes, ejemplos incluyen el Tiempo Medio de Resolución (MTTR) y el porcentaje de cumplimiento de SLA.
- **Tiempo Medio de Resolución (MTTR):** El MTTR es el promedio de tiempo requerido para resolver un incidente desde su registro hasta su cierre. Es un indicador clave para evaluar la eficiencia del proceso de soporte técnico.
- **Service Desk:** El Service Desk es el punto único de contacto entre los usuarios y el departamento de TI, encargado de registrar, gestionar y canalizar incidentes y solicitudes de servicio.
- **Base de Datos de Configuración (CMDB):** La CMDB es un repositorio estructurado que contiene información sobre los activos de TI y sus relaciones. Permite analizar el impacto de incidentes y cambios sobre los componentes tecnológicos.
- **Riesgo Tecnológico:** El riesgo tecnológico se refiere a la posibilidad de que fallos en los sistemas de información afecten la continuidad operativa, la seguridad o el cumplimiento normativo de una organización.
- **Trazabilidad:** La trazabilidad es la capacidad de rastrear un incidente o cambio desde su origen hasta su resolución, manteniendo evidencia documental de cada etapa del proceso.
- **Mejora Continua:** La mejora continua es el proceso sistemático de evaluación y optimización de procesos y servicios, basado en el análisis de indicadores y retroalimentación organizacional.
- **Sistema de Gestión de Servicios (SGS):** El Sistema de Gestión de Servicios es el conjunto estructurado de políticas, procesos y controles implementados para planificar, operar y mejorar los servicios de TI, conforme a estándares como ISO/IEC 20000.

2.7. MARCO LEGAL

2.7.1. MARCO LEGAL NACIONAL

2.7.1.1. LEY DEL SISTEMA FINANCIERO (DECRETO NO. 129-2004)

La Ley del Sistema Financiero de Honduras (Decreto No. 129-2004) constituye el marco jurídico principal que regula la organización, funcionamiento y supervisión de las instituciones

financieras en el país. Esta normativa establece los principios estructurales bajo los cuales deben operar los bancos, incluyendo disposiciones relacionadas con solvencia, administración de riesgos y control interno. (República de Honduras, 2004)

El sistema financiero hondureño se rige principalmente por la Ley del Sistema Financiero (Decreto No. 129-2004). La República de Honduras (2004) establece en su artículo 1 que las instituciones deben brindar un servicio transparente, sólido y confiable (pág. 2). Esta disposición permite identificar los principios de transparencia y solidez como pilares estructurales del sistema financiero nacional.

Asimismo, la República de Honduras (2004) dispone en el artículo 2 que la intermediación financiera es una actividad de interés público (pág. 2) lo que implica que la actividad bancaria está sujeta a supervisión estatal permanente.

En materia de solvencia patrimonial, la República de Honduras (2004) establece en el artículo 37 la obligación de mantener índices de adecuación de capital acordes a los riesgos asumidos por la institución (pág. 14). Esta exigencia busca garantizar respaldo financiero suficiente frente a pérdidas potenciales.

Adicionalmente, el artículo 73 de la Ley del Sistema Financiero exige la implementación de procesos integrales de administración de riesgos y sistemas de control interno adecuados, lo que constituye el fundamento legal de la gestión prudente de riesgos dentro del sistema financiero hondureño. (República de Honduras, 2004, pág. 26)

Estos principios constituyen la base normativa sobre la cual se estructura la supervisión bancaria en el país:



Figura 14: Principios fundamentales de la regulación bancaria hondureña

Fuente: Elaboración propia con base en la Ley del Sistema Financiero de Honduras (2004).

El esquema muestra cinco pilares principales:

- **Transparencia:** implica la obligación de las instituciones financieras de proporcionar información clara, veraz y oportuna, fortaleciendo la confianza del público y del mercado.
- **Solidez financiera:** se refiere a la estabilidad estructural de las entidades bancarias, asegurando que cuenten con bases financieras firmes para operar de manera sostenible.
- **Solvencia patrimonial:** garantiza que las instituciones mantengan niveles adecuados de capital para respaldar sus riesgos y cumplir con sus obligaciones.
- **Administración prudente de riesgos:** destaca la importancia de identificar, medir, controlar y monitorear los riesgos financieros, operativos y tecnológicos de forma preventiva.
- **Control interno efectivo:** asegura la existencia de mecanismos adecuados de supervisión, auditoría y cumplimiento normativo dentro de las entidades.

2.7.1.2. COMISIÓN NACIONAL DE BANCOS Y SEGUROS (CNBS)

La Comisión Nacional de Bancos y Seguros (CNBS) constituye el ente supervisor responsable de la regulación y supervisión prudencial del sistema financiero hondureño. Su

función principal es garantizar que las instituciones supervisadas operen conforme al marco normativo vigente, manteniendo estabilidad financiera, solvencia patrimonial y adecuada gestión de riesgos.

De conformidad con la Ley del Sistema Financiero, la CNBS posee facultades técnicas y sancionatorias que le permiten ejercer control sobre las entidades reguladas (República de Honduras, 2004). Entre sus atribuciones se encuentra la emisión de normas prudenciales obligatorias, mediante las cuales se establecen lineamientos técnicos y regulatorios que deben cumplir las instituciones financieras.

Asimismo, la CNBS tiene la facultad de supervisar el cumplimiento regulatorio a través de mecanismos de vigilancia permanente, lo que incluye la realización de inspecciones tanto in situ como extra situ. Estas modalidades de supervisión permiten evaluar la situación financiera, la calidad de los activos, el cumplimiento de índices patrimoniales y la efectividad de los sistemas de control interno.

Con el propósito de sintetizar las principales atribuciones del ente supervisor, se presenta a continuación un esquema conceptual de las facultades que la Ley del Sistema Financiero otorga a la Comisión Nacional de Bancos y Seguros.

Estas son las facultades permitidas a la comisión Nacional de Banca y Seguros (CNBS):



Figura 15: Facultades de la Comisión Nacional de Bancos y Seguros

Fuente: Elaboración propia con base en la Ley del Sistema Financiero de Honduras (2004).

En el centro se ubica la CNBS, y alrededor se muestran sus atribuciones fundamentales:

- **Emitir normas prudenciales obligatorias:** establecer regulaciones que las instituciones financieras deben cumplir para garantizar estabilidad, solvencia y adecuada gestión de riesgos.
- **Realizar inspecciones in situ y extra situ:** llevar a cabo supervisiones directas en las entidades (in situ) y revisiones documentales o análisis externos (extra situ) para verificar el cumplimiento normativo.
- **Solicitar reportes periódicos:** exigir información financiera, operativa y de riesgos de manera continua para monitorear la situación de las instituciones.
- **Imponer sanciones administrativas:** aplicar medidas correctivas o sanciones cuando se detecten incumplimientos regulatorios.
- **Exigir planes de acción correctiva:** requerir a las entidades la implementación de medidas específicas para subsanar debilidades identificadas.
- **Supervisar la gestión de riesgos:** verificar que las instituciones administren adecuadamente los riesgos financieros, operativos, tecnológicos y de mercado.

En consecuencia, el marco regulatorio hondureño ha evolucionado desde un enfoque prudencial tradicional hacia una supervisión que incorpora de manera explícita la dimensión tecnológica, sentando las bases para el análisis específico del riesgo tecnológico en banca.

2.7.1.3. RESOLUCIÓN NO. 025-2022 – NORMAS PARA LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD DEL NEGOCIO

La regulación específica del riesgo tecnológico se consolida con la emisión de la Resolución No. 025-2022, mediante la cual la Comisión Nacional de Bancos y Seguros aprueba las Normas para la Gestión de Tecnologías de Información, Ciberseguridad y Continuidad del Negocio.

Dicha normativa establece que las instituciones supervisadas deben implementar un marco formal de gestión tecnológica que garantice:

- Seguridad de la información
- Gestión de ciberseguridad
- Continuidad del negocio
- Gestión de proveedores tecnológicos
- Monitoreo de infraestructura crítica

La normativa señala expresamente que su objeto es regular la gestión de tecnologías de información y fortalecer la seguridad y continuidad operativa en las instituciones supervisadas (Comisión Nacional de Bancos y Seguros, 2022)

Este desarrollo regulatorio evidencia una evolución desde un modelo prudencial tradicional hacia uno que integra explícitamente el riesgo tecnológico como componente esencial de la estabilidad financiera.

2.7.1.4. RIESGO OPERACIONAL Y RIESGO TECNOLÓGICO EN EL SISTEMA FINANCIERO

El riesgo tecnológico es considerado, dentro del riesgo operacional, como la posibilidad de pérdidas derivadas de fallas en sistemas, procesos tecnológicos o eventos externos que afecten la infraestructura digital de la institución financiera (Comisión Nacional de Bancos y Seguros, 2022).

En el contexto hondureño, aunque la Ley del Sistema Financiero (2004) no emplea expresamente el término “riesgo tecnológico”, sí establece obligaciones que constituyen su fundamento jurídico. En particular, el artículo 37 dispone que las instituciones deben mantener un índice de adecuación de capital acorde a los riesgos asumidos y a la eficacia de los procesos con los que los gestionan y controlan (Ley del Sistema Financiero, Decreto No. 129-2004, pág. 16).

Estas disposiciones permiten interpretar que el marco legal hondureño incorpora el principio de gestión integral de riesgos, dentro del cual el riesgo tecnológico queda comprendido como parte del riesgo operacional.

Con el propósito de evidenciar la relación entre el marco legal general y el desarrollo técnico especializado en materia tecnológica, se presenta a continuación un cuadro comparativo entre la Ley del Sistema Financiero y la Resolución No. 025-2022.

A continuación, se muestra una tabla comparativa entre la Ley del sistema financiero y la Resolución No. No. 025-2022:

Tabla 9: Comparación entre la Ley del Sistema Financiero y la Resolución No. 025-2022

Criterio de análisis	Ley del Sistema Financiero (2004)	Resolución No. 025-2022 (CNBS, 2022)
Naturaleza jurídica	Ley marco de carácter general que regula la organización, funcionamiento y supervisión del sistema financiero.	Norma técnica específica emitida por la CNBS para regular la gestión tecnológica.
Enfoque regulatorio	Gestión integral de riesgos financieros y prudenciales.	Gestión específica del riesgo tecnológico y digital.
Base legal de gestión de riesgos	Art. 30: Responsabilidad del Consejo en la administración de riesgos (República de Honduras, 2004, p. 12).	Establece estructura formal para gestión de TI, seguridad y continuidad (CNBS, 2022).
Adecuación de capital y riesgos	Art. 37: Índices de adecuación de capital acordes a los riesgos asumidos (p. 16).	No regula capital, sino controles tecnológicos preventivos.
Control interno	Art. 73: Obligación de procesos integrales de administración de riesgos y control interno (p. 26).	Define controles específicos de seguridad de la información y ciberseguridad.
Continuidad operativa	Implícita dentro del deber de gestión prudente de riesgos.	Regula expresamente planes de continuidad del negocio y recuperación ante desastres.
Seguridad de la información	No desarrollada técnicamente.	Regula explícitamente políticas, controles y monitoreo de seguridad de la información.
Gestión de proveedores tecnológicos	No desarrolla regulación específica sobre terceros tecnológicos.	Exige evaluación y supervisión formal de proveedores tecnológicos.
Supervisión	CNBS con facultades generales de supervisión prudencial.	CNBS con enfoque técnico especializado en supervisión tecnológica.
Objetivo final	Estabilidad, solvencia y protección del público depositante (Art. 1 y 2, p. 2).	Fortalecer seguridad digital, continuidad operativa y resiliencia tecnológica.

Fuente: Elaboración propia con base en la Ley del Sistema Financiero (República de Honduras, 2004) y la Resolución No. 025-2022 de la CNBS (2022).

El análisis del marco legal nacional evidencia que las instituciones financieras en Honduras no solo deben operar con solvencia financiera, sino también demostrar control efectivo sobre sus riesgos tecnológicos y operativos.

La propuesta de formalización de la gestión de incidencias de software en Banco Ficensa se alinea con:

- La obligación de control interno establecida en la Ley del Sistema Financiero.
- La exigencia de administración integral de riesgos.
- Las Normas de Gestión Tecnológica y Continuidad del Negocio emitidas por la CNBS.
- La necesidad de garantizar disponibilidad y resiliencia de servicios financieros críticos.

De esta manera, la propuesta no se presenta como una iniciativa aislada de mejora

2.7.1.5. GOBIERNO CORPORATIVO Y GESTIÓN DEL RIESGO TECNOLÓGICO EN EL MARCO REGULATORIO HONDUREÑO

La gestión del riesgo tecnológico no constituye una responsabilidad exclusiva del área de tecnología, sino que forma parte de las obligaciones del Consejo de Administración y de la alta gerencia.

El artículo 30 establece que el Consejo de Administración debe velar por la implementación de políticas, sistemas y procesos necesarios para la correcta administración y control de los riesgos inherentes al negocio (Ley del Sistema Financiero, Decreto No. 129-2004, pág. 12). Esta disposición incluye, por interpretación sistemática, el riesgo tecnológico como parte del riesgo operacional.

Por su parte, la Resolución No. 025-2022 exige la existencia de una estructura formal de gobierno de tecnologías de información, con responsabilidades claramente definidas y mecanismos de supervisión interna (Comisión Nacional de Bancos y Seguros, 2022).

Esto implica que:

- El Consejo debe aprobar políticas de gestión tecnológica.
- La alta gerencia debe garantizar recursos adecuados.
- Deben existir comités o instancias de supervisión tecnológica.
- La auditoría interna debe evaluar controles tecnológicos.

La incorporación del riesgo tecnológico dentro del esquema de gobierno corporativo fortalece la resiliencia institucional y reduce la exposición a eventos disruptivos.

Posteriormente, se presenta la estructura de gobierno para la gestión del riesgo tecnológico, conforme a lo establecido en la Ley del Sistema Financiero y en la Resolución No.

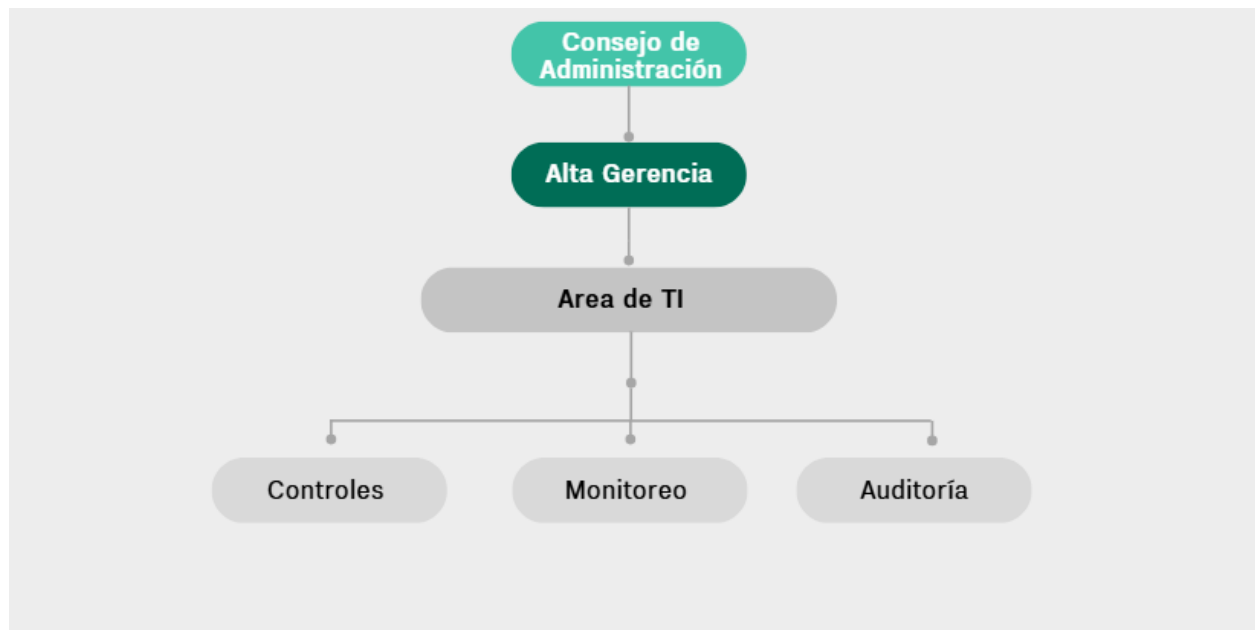


Figura 16: Estructura de gobierno en la gestión del riesgo tecnológico

Fuente: Elaboración propia con base en la Ley del Sistema Financiero (República de Honduras, 2004) y la Resolución No. 025-2022 de la CNBS (2022).

2.7.1.6. VINCULACIÓN DEL MARCO LEGAL CON LA PROPUESTA

El análisis del marco legal nacional evidencia que las instituciones financieras en Honduras no solo deben operar con solvencia financiera, sino también demostrar control efectivo sobre sus riesgos tecnológicos y operativos.

La propuesta de formalización de la gestión de incidencias de software en Banco Ficensa se alinea con:

- La obligación de control interno establecida en la Ley del Sistema Financiero.
- La exigencia de administración integral de riesgos.
- Las Normas de Gestión Tecnológica y Continuidad del Negocio emitidas por la CNBS.
- La necesidad de garantizar disponibilidad y resiliencia de servicios financieros críticos.

En consecuencia, la formalización de la gestión de incidencias de software no constituye únicamente una mejora operativa, sino una obligación implícita derivada del marco regulatorio prudencial hondureño.

3. CAPÍTULO III. METODOLOGÍA DE LA INVESTIGACIÓN

3.1.ENFOQUE

El enfoque cuantitativo se caracteriza por utilizar la medición numérica y el análisis estadístico para describir fenómenos y establecer patrones dentro de una población determinada. Este enfoque permite examinar los datos de manera objetiva y estructurada con el propósito de generar conclusiones basadas en evidencia empírica (Hernández Sampieri y otros, 2014).

La presente investigación se desarrolla bajo un enfoque cuantitativo, ya que se basa en la recopilación, organización y análisis de datos numéricos relacionados con las incidencias de software que afectan a las áreas de Negocios y Operaciones de Banco Ficensa durante el año 2025.

El análisis se realiza a partir de los registros de incidencias identificados en correos electrónicos, comunicaciones internas y reportes operativos del área de tecnología, los cuales serán consolidados en una base de datos estructurada para su análisis.

En este contexto, la investigación se enfoca principalmente en analizar información cuantificable proveniente de los registros de incidencias de software reportadas en el Banco Ficensa durante el año 2025. A partir de estos datos se calcularán indicadores como frecuencia de incidencias, tiempos promedio de atención y resolución, clasificación por criticidad y porcentaje de incidencias registradas formalmente.

Posteriormente, con base en los resultados obtenidos del análisis cuantitativo, se plantea el diseño de un flujo formal de gestión de incidencias alineado con las buenas prácticas de gestión de servicios de TI. Este tipo de propuestas es común en investigaciones aplicadas en el ámbito organizacional, donde el diagnóstico cuantitativo permite fundamentar la formulación de mejoras o modelos de gestión dentro de una institución.

3.2.ALCANCE

El alcance de la presente investigación es descriptivo, ya que tiene como propósito analizar la gestión de las incidencias de software que afectan a las áreas de Negocios y Operaciones del Banco Ficensa.

De acuerdo con Hernández Sampieri, Fernández Collado y Baptista Lucio, los estudios descriptivos tienen como finalidad detallar las características de un fenómeno o situación

específica dentro de un contexto determinado. En este sentido, los autores señalan que “los estudios descriptivos buscan especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis” (Hernández Sampieri y otros, 2014).

A través del estudio se pretende identificar aspectos como:

- Frecuencia de las incidencias de software.
- Tiempos de atención y resolución de las incidencias.
- Clasificación de las incidencias según su tipo o criticidad.
- Percepción de los usuarios sobre la gestión de incidencias.

El análisis de estos elementos permitirá comprender la situación actual del manejo de incidencias de software dentro de la organización y generar información que sirva de base para el diseño de una propuesta de mejora alineada con las buenas prácticas de gestión de incidencias establecidas en ITIL 4.

3.3. DISEÑO DE INVESTIGACIÓN, POBLACIÓN Y MUESTRA

3.3.1. DISEÑO

La investigación adopta un diseño no experimental, debido a que las variables de estudio no serán manipuladas por los investigadores, sino que se analizarán tal como ocurren dentro del entorno organizacional de Banco Ficensa. En este tipo de diseño, los fenómenos se observan en su contexto natural sin que exista intervención directa sobre las variables de estudio (Hernández Sampieri y otros, 2014).

Asimismo, el estudio presenta un diseño transversal, ya que el análisis se realizará sobre información correspondiente al año 2025, considerando las incidencias de software registradas durante dicho período. Los estudios transversales se caracterizan porque “recolectan datos en un solo momento, en un tiempo único. Su propósito es describir variables y analizar su incidencia e interrelación en un momento dado” (Hernández Sampieri y otros, 2014, pág. 184).

3.3.2. POBLACIÓN

La población se entiende como “el conjunto de todos los casos que concuerdan con determinadas especificaciones” (Hernández Sampieri y otros, 2014, pág. 204).

La población del estudio está conformada por dos tipos de unidades de análisis: los usuarios de los sistemas tecnológicos de Banco Ficensa y los registros de incidencias de software generados dentro de la organización.

Por una parte, la población relacionada con los usuarios está conformada por los empleados de Banco Ficensa que utilizan el software desarrollado internamente y reportan incidencias, conformados principalmente por las áreas de Negocios y Operaciones, quienes utilizan los sistemas tecnológicos en el desarrollo de sus actividades laborales y reportan incidencias relacionadas con el funcionamiento de las aplicaciones.

Por otra parte, la investigación también considera como población los registros de incidencias de software reportadas en los sistemas tecnológicos del Banco Ficensa durante el año 2025, los cuales serán analizados para identificar la frecuencia de incidencias, tiempos de atención, tiempos de resolución y clasificación según tipo o criticidad.

Banco Ficensa cuenta con un total de 303 empleados. La población objetivo del estudio quedó conformada por 110 colaboradores usuarios del software desarrollado internamente por el banco que reportan incidencias durante el desarrollo de sus funciones. De estos, 97 pertenecen a las áreas de Negocios y Operaciones y 13 corresponden a colaboradores de otras áreas que utilizan sistemas regulatorios desarrollados internamente y reportan incidencias de software, por lo que comparten la condición esencial que define la unidad de análisis. La delimitación se sustenta en el uso efectivo del software interno y no en la adscripción administrativa del colaborador, lo que asegura que la totalidad de la población objetivo experimenta directamente el fenómeno estudiado.

3.3.3. TÉCNICAS DE MUESTREO

El muestreo es el proceso mediante el cual se selecciona una parte de la población con el propósito de analizar sus características y obtener información sobre el fenómeno estudiado (Hernández Sampieri y otros, 2014).

En el presente estudio se utiliza un muestreo no probabilístico, el cual se caracteriza porque la selección de los elementos de la muestra no depende de la probabilidad, sino de criterios

definidos por el investigador en función de los objetivos de la investigación. Según Hernández Sampieri, Fernández Collado y Baptista Lucio, “la elección de los elementos no depende de la probabilidad sino de las características de la investigación” (Hernández Sampieri y otros, 2014, pág. 226).

Dentro de este tipo de muestreo se aplica un muestreo censal, el cual consiste en incluir la totalidad de los elementos que conforman la población objetivo dentro del estudio. Este tipo de muestreo se utiliza cuando el tamaño de la población es reducido y accesible, lo que permite analizar todos los casos que presentan las características requeridas para la investigación.

En el caso de la presente investigación, la población objetivo está conformada por 110 colaboradores usuarios del software interno del banco mayormente pertenecientes a las áreas de Negocios y Operaciones de Banco Ficensa, quienes utilizan los sistemas tecnológicos en el desarrollo de sus actividades laborales y reportan incidencias relacionadas con el funcionamiento de las aplicaciones.

Debido a que el tamaño de la población objetivo es reducido y accesible para el proceso de recolección de datos, se incluyen los 110 usuarios que conforman la población objetivo, aplicando así un muestreo censal, lo que permite analizar la totalidad de los elementos que conforman la población objetivo del estudio.

3.3.4. MUESTRA

De acuerdo con Hernández Sampieri, Fernández Collado y Baptista Lucio, una muestra es “un subgrupo de la población de interés sobre el cual se recolectarán los datos y que debe ser representativo de dicha población” (Hernández Sampieri y otros, 2014, pág. 212).

La muestra del estudio se obtiene a partir de la aplicación de un muestreo no probabilístico de tipo censal, el cual consiste en incluir la totalidad de los elementos que conforman la población objetivo dentro del proceso de investigación.

En el Banco Ficensa existe una población total de 303 empleados. Sin embargo, el estudio se enfoca en los colaboradores usuarios del software interno del banco, conformados principalmente por Negocios y Operaciones, debido a que estos usuarios interactúan directamente con los sistemas tecnológicos y reportan incidencias de software durante el desarrollo de sus funciones.

Por lo tanto, al aplicar un muestreo censal, la muestra queda conformada por los 110 empleados pertenecientes a las áreas de Negocios y Operaciones del Banco Ficensa, quienes participan en la aplicación del cuestionario para recopilar información sobre su percepción respecto a la gestión de incidencias de software.

De manera adicional, se analizan los registros de incidencias de software correspondientes al período 2025, los cuales permiten evaluar aspectos como la frecuencia de los incidentes, los tiempos de atención y resolución, así como su clasificación según tipo o impacto dentro de la organización.

3.4.CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

Para el desarrollo de la investigación se establecieron criterios que permiten delimitar qué información será considerada dentro del análisis de la gestión de incidencias de software en Banco Ficensa. Los mismos se detallan en la siguiente tabla:

Tabla 10: Criterios de inclusión y exclusión

Criterios de inclusión	Criterios de exclusión
Incidencias relacionadas con software o aplicaciones utilizadas en el Banco Ficensa.	Incidencias relacionadas con fallas de hardware.
Incidencias reportadas por usuarios de las áreas de Negocios y Operaciones.	Problemas asociados a infraestructura de red o telecomunicaciones reportados por otras áreas.
Incidencias reportadas al área de tecnología mediante correos electrónicos, comunicaciones internas o reportes operativos.	Solicitudes de servicio o requerimientos que no correspondan a incidencias de software.
Incidencias registradas durante el período de análisis definido para la investigación.	Registros que no cuenten con información suficiente para su análisis.

Fuente: Elaboración propia

Estos criterios permiten delimitar el alcance del estudio y asegurar que el análisis se centre únicamente en las incidencias de software que afectan las áreas de Negocios y Operaciones del Banco Ficensa.

3.5. ESQUEMA DE VARIABLES

Para el desarrollo de la investigación se definieron dos variables descriptivas que permiten analizar la gestión de incidencias de software en las áreas de Negocios y Operaciones de Banco FICENSA durante el año 2025.

Las variables representan características o propiedades que pueden variar y que son susceptibles de ser observadas o medidas dentro de una investigación. De acuerdo con Hernández

Sampieri, Fernández Collado y Baptista Lucio, una variable es “una propiedad que puede variar y cuya variación es susceptible de medirse u observarse” (Hernández Sampieri y otros, 2014).

La primera variable corresponde a la gestión de incidencias de software, entendida como el conjunto de actividades relacionadas con el registro, clasificación, priorización, seguimiento, resolución y cierre de las incidencias dentro de la organización.

La segunda variable corresponde a la eficiencia operativa del proceso de atención de incidencias, relacionada con el desempeño observado mediante los tiempos de atención y resolución, la reincidencia, el cumplimiento de criterios de seguimiento y la percepción de los usuarios.

Ambas variables se analizan de manera complementaria para describir la situación actual del proceso. La investigación no pretende comprobar que una variable produce cambios en la otra ni establecer una relación causal entre ellas.

A partir de estas variables se establecieron dimensiones e indicadores que permiten organizar la información obtenida mediante la matriz documental y el cuestionario de percepción.

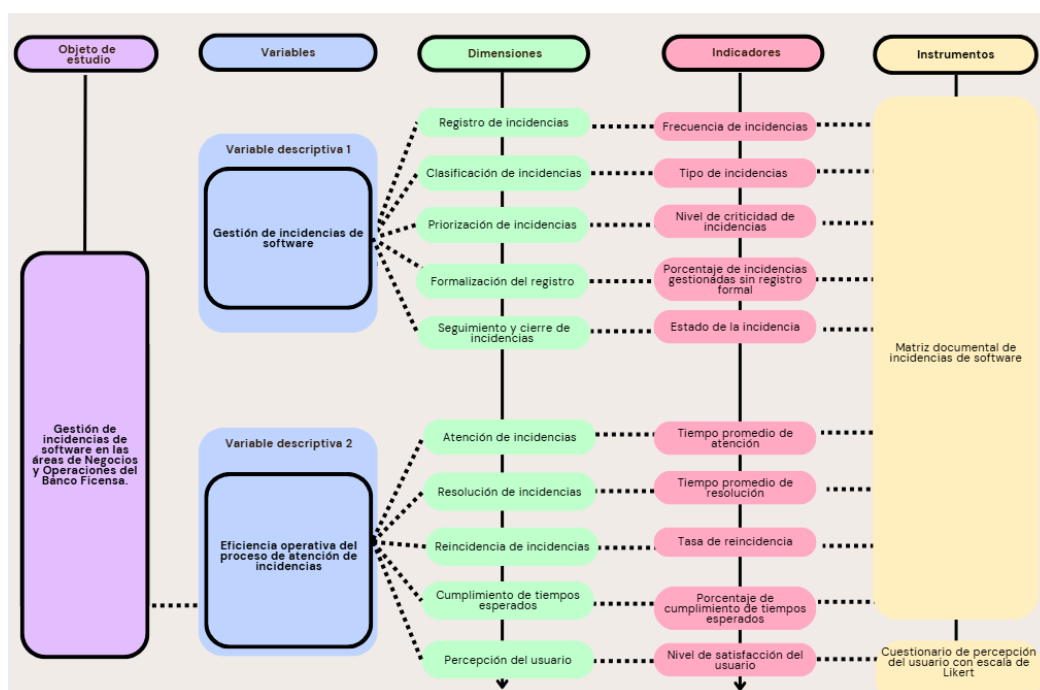


Figura 17: Esquema de las variables del estudio

Fuente: Elaboración propia.

3.6. OPERACIONALIZACIÓN DE VARIABLES

La operacionalización permite transformar los conceptos centrales de la investigación en dimensiones e indicadores observables y medibles. En el presente estudio se consideran dos variables descriptivas: la gestión de incidencias de software y la eficiencia operativa del proceso de atención de incidencias.

La gestión de incidencias de software se analiza mediante las actividades de registro, clasificación, priorización, formalización, seguimiento y cierre. Sus indicadores permiten describir la frecuencia de las incidencias, los tipos registrados, los niveles de criticidad, la formalización del registro y el estado de los casos.

La eficiencia operativa del proceso de atención se analiza mediante indicadores relacionados con los tiempos de atención y resolución, la reincidencia, el cumplimiento de los tiempos esperados y la percepción del usuario respecto al servicio recibido.

Ambas variables se examinan de forma descriptiva y complementaria. La investigación no establece una relación de dependencia ni pretende demostrar que una variable causa modificaciones en la otra.

Esta operacionalización responde al enfoque cuantitativo y descriptivo del estudio. Su aplicación permite caracterizar las incidencias de software identificadas durante 2025 y establecer una línea base para el diseño del modelo basado en ITIL 4.

Tabla 11: Operacionalización de variables descriptivas

Variable	Conceptualización	Definición operacional	Dimensión	Indicador	Fórmula o criterio de medición	Fuente	Instrumento
Gestión de incidencias de software	Conjunto de actividades orientadas al registro, clasificación, priorización, seguimiento, resolución y cierre de las incidencias de software que afectan a Negocios y Operaciones.	Se analizarán las incidencias identificadas durante 2025, considerando su frecuencia, tipo, criticidad, área afectada, medio de registro y estado de gestión.	Registro de incidencias	Frecuencia de incidencias	Total de incidencias identificadas durante el período. También podrá calcularse mensualmente: número de incidencias por mes.	Correos electrónicos, reportes internos, bitácoras operativas y registros del área de Tecnología.	Matriz documental de incidencias de software.
	Conjunto de actividades orientadas al registro, clasificación, priorización, seguimiento, resolución y cierre de las incidencias de software que afectan a Negocios y Operaciones.	Se analizará la clasificación asignada a cada incidencia de acuerdo con la naturaleza de la falla o afectación reportada.	Clasificación de incidencias	Tipo de incidencias registradas	Clasificación según las categorías definidas: falla funcional, error, integración, datos incorrectos u otra categoría aplicable.	Correos electrónicos, reportes internos, bitácoras operativas y registros del área de Tecnología.	Matriz documental de incidencias de software.

Variable	Conceptualización	Definición operacional	Dimensión	Indicador	Fórmula o criterio de medición	Fuente	Instrumento
	Conjunto de actividades orientadas al registro, clasificación, priorización, seguimiento, resolución y cierre de las incidencias de software que afectan a Negocios y Operaciones.	Se analizará el nivel de criticidad asignado a cada incidencia según su impacto en los procesos del negocio.	Priorización de incidencias	Nivel de criticidad	Clasificación según criticidad alta, media o baja, considerando el impacto operativo, los usuarios afectados y la afectación de procesos críticos.	Correos electrónicos, reportes internos, bitácoras operativas y registros del área de Tecnología.	Matriz documental de incidencias de software.
	Conjunto de actividades orientadas al registro, clasificación, priorización, seguimiento, resolución y cierre de las incidencias de software que afectan a Negocios y Operaciones.	Se verificará si las incidencias cuentan con evidencia documental suficiente para dar seguimiento a su ciclo de vida.	Formalización del registro	Porcentaje de incidencias gestionadas sin registro formal	$\left(\frac{\text{Incidencias sin registro formal}}{\text{Total de incidencias identificadas}} \right) \times 100.$	Correos electrónicos, reportes internos, bitácoras operativas y registros del área de Tecnología.	Matriz documental de incidencias de software.
	Conjunto de actividades orientadas al registro, clasificación, priorización, seguimiento, resolución y cierre de las incidencias de software que afectan a Negocios y Operaciones.	Se analizará el estado final de cada incidencia y la existencia de evidencia de seguimiento, resolución o cierre.	Seguimiento y cierre	Estado de la incidencia	Clasificación del estado: abierta, en proceso, resuelta o cerrada. También se verificará la existencia de evidencia de seguimiento y cierre.	Correos electrónicos, reportes internos, bitácoras operativas y registros del área de Tecnología.	Matriz documental de incidencias de software.

Variable	Conceptualización	Definición operacional	Dimensión	Indicador	Fórmula o criterio de medición	Fuente	Instrumento
Eficiencia operativa del proceso de atención de incidencias	Características del desempeño observado en la atención y resolución de incidencias de software, considerando oportunidad, trazabilidad y control.	Se analizarán indicadores cuantitativos obtenidos de los registros documentales para describir los tiempos de atención de las incidencias.	Atención de incidencias	Tiempo promedio de atención	Suma de los tiempos de atención / Total de incidencias con datos completos. Tiempo de atención = Fecha y hora de inicio de atención – Fecha y hora del reporte.	Correos electrónicos, reportes internos, bitácoras operativas y registros del área de Tecnología.	Matriz documental de incidencias de software.
	Características del desempeño observado en la atención y resolución de incidencias de software, considerando oportunidad, trazabilidad y control.	Se calculará el tiempo transcurrido entre el reporte de la incidencia y su resolución documentada.	Resolución de incidencias	Tiempo promedio de resolución	Suma de los tiempos de resolución / Total de incidencias resueltas con datos completos. Tiempo de resolución = Fecha y hora de resolución – Fecha y hora del reporte.	Correos electrónicos, reportes internos, bitácoras operativas y registros del área de Tecnología.	Matriz documental de incidencias de software.

Variable	Conceptualización	Definición operacional	Dimensión	Indicador	Fórmula o criterio de medición	Fuente	Instrumento
	Características del desempeño observado en la atención y resolución de incidencias de software, considerando oportunidad, trazabilidad y control.	Se identificarán las incidencias repetidas asociadas con un mismo sistema, módulo, proceso o causa aparente durante 2025.	Reincidencia de incidencias	Tasa de reincidencia	$(\text{Incidencias reincidentes} / \text{Total de incidencias identificadas}) \times 100.$	Correos electrónicos, reportes internos, bitácoras operativas y registros del área de Tecnología.	Matriz documental de incidencias de software.
	Características del desempeño observado en la atención y resolución de incidencias de software, considerando oportunidad, trazabilidad y control.	Se medirá después de incorporar formalmente las incidencias a la Mesa de Servicio y establecer tiempos objetivo según su criticidad.	Cumplimiento de tiempos esperados	Cumplimiento de SLA	$(\text{Incidencias gestionadas dentro del SLA} / \text{Total de incidencias evaluadas}) \times 100.$	Registros generados por la Mesa de Servicio después de la implementación.	Reportes de ManageEngine ServiceDesk Plus.

Variable	Conceptualización	Definición operacional	Dimensión	Indicador	Fórmula o criterio de medición	Fuente	Instrumento
	Características del desempeño observado en la atención y resolución de incidencias de software, considerando oportunidad, trazabilidad y control.	Se analizará la percepción de los usuarios de Negocios y Operaciones sobre la atención, seguimiento, comunicación y resolución de las incidencias.	Percepción del usuario	Nivel de satisfacción del usuario	Promedio de las respuestas obtenidas mediante la escala de Likert.	Usuarios de las áreas de Negocios y Operaciones.	Cuestionario de percepción del usuario.

Fuente: Elaboración propia.

3.7.TÉCNICAS, INSTRUMENTOS, PROCEDIMIENTOS Y PLAN DE ANÁLISIS

Para el desarrollo de la presente investigación se emplearon técnicas e instrumentos de recolección de información orientados al análisis de la gestión de incidencias de software en las áreas de Negocios y Operaciones de Banco Ficensa.

3.7.1. TÉCNICAS

La recolección de los datos implica elaborar un plan detallado de procedimientos que conduzcan a reunir información con un propósito específico para el estudio. El investigador se auxilia de diversas técnicas que se desarrollan para medir las variables de interés de forma confiable y válida, permitiendo comprender y dimensionar la problemática organizacional (Hernández Sampieri y otros, 2014). Para esta investigación, orientada a fundamentar la necesidad de una Mesa de Servicio alineada a ITIL 4 en Banco Ficensa, se emplearon las siguientes técnicas:

- **Encuestas:** Implican la formulación de un conjunto de preguntas predefinidas que se administran de manera uniforme a un grupo de participantes. Esta técnica permite recopilar datos cuantitativos sobre diversos aspectos de una población (Hernández Sampieri y otros, 2014). En el presente proyecto, la encuesta se aplicó a los colaboradores usuarios del software interno del banco, con el objetivo de cuantificar sus percepciones, el nivel de satisfacción actual, y evaluar los tiempos de respuesta del departamento de TI frente a la gestión de incidentes de software y solicitudes de servicio.
- **Análisis documental:** Es una técnica de recolección que consiste en la detección, obtención y consulta de materiales o registros institucionales donde se agrupa información de interés para el análisis de un fenómeno (Hernández Sampieri y otros, 2014, pág. 314). Esta técnica se empleó para examinar la información histórica del año 2025 proveniente de los canales de comunicación descentralizados que actualmente utilizan los usuarios (correos electrónicos, registros de llamadas telefónicas y mensajes directos vía Teams y WhatsApp). Su aplicación fue fundamental para determinar el volumen real de solicitudes ingresadas, evidenciar la falta de trazabilidad en los tickets y justificar la urgencia de centralizar la operación.

3.7.2. INSTRUMENTOS

Según Hernández Sampieri y Fernández Collado (2014), un instrumento de recolección de datos es cualquier recurso que utiliza el investigador para registrar la información relacionada con el fenómeno estudiado, permitiendo medir o describir las variables de interés de forma organizada. Para el desarrollo de la presente investigación se utilizaron los siguientes instrumentos de recolección de información:

Cuestionario de percepción del usuario (escala de Likert): Se diseñó un cuestionario digital estructurado con escala tipo Likert, dirigido al censo de colaboradores usuarios del software interno del banco. Este instrumento está integrado por preguntas cerradas que permiten obtener información estandarizada para medir numéricamente la percepción del usuario respecto a la gestión actual de incidencias de software, considerando dimensiones como tiempos de respuesta y resolución, seguimiento y trazabilidad, efectividad del soporte, satisfacción general y aceptación de una Mesa de Servicio centralizada. Este instrumento aporta de forma directa al objetivo orientado a determinar la percepción del usuario sobre la gestión actual de incidencias de software. ([Ver Anexo 4](#)).

Matriz de recolección de datos documentales: Es un instrumento estructurado en formato de base de datos que se utilizará para llevar a cabo el análisis documental de las incidencias y solicitudes relacionadas con los servicios de TI. Esta matriz permitirá la extracción, categorización y sistematización de los registros históricos del año 2025 provenientes de los múltiples canales de comunicación descentralizados (correos electrónicos, llamadas telefónicas, Teams y WhatsApp). El instrumento incluye campos específicos para clasificar la fecha de la solicitud, el canal de recepción, el tipo de requerimiento (incidente o solicitud de servicio) y la existencia de trazabilidad, permitiendo evidenciar empíricamente las áreas de ineficiencia y las discrepancias operativas que justifican la implementación de ITIL 4. ([Ver Anexo 5](#)).

Tabla 12: Vinculación Objetivos/Instrumentos

Objetivo específico	Instrumento	Tipo de dato
Analizar la situación actual de la gestión de incidencias de software en las áreas de Negocios y Operaciones de Banco Ficensa durante el año 2025, con base en el registro, la trazabilidad, la frecuencia de ocurrencia y el control operativo de los casos reportados.	Cuestionario de percepción del usuario con escala Likert; Matriz Documental de Incidencias de Software 2025; Matriz de Evaluación de Capacidad del Proceso basada en COBIT 2019; e Indicadores Clave de Desempeño (KPIs).	Datos de percepción de los usuarios; registros históricos de incidencias; evidencia documental sobre trazabilidad, formalización del registro y control operativo; valoración del nivel actual de capacidad del proceso; y resultados consolidados de la línea base de indicadores.
Calcular el tiempo promedio de atención y resolución de las incidencias de software registradas en el año 2025 en Banco Ficensa.	Matriz Documental de Incidencias de Software 2025 e Indicadores Clave de Desempeño (KPIs).	Registros históricos de fechas de reporte, primera atención y resolución; tiempo promedio de atención; y tiempo promedio de resolución de los casos cerrados.
Clasificar y cuantificar las incidencias de software según tipo, criticidad y área afectada durante el año 2025 en Banco Ficensa.	Matriz Documental de Incidencias de Software 2025.	Registros históricos clasificados según tipo de incidencia, nivel de criticidad, área funcional afectada y sistema involucrado.
Determinar el porcentaje de incidencias de software gestionadas sin registro formal durante el año 2025 en Banco Ficensa.	Matriz Documental de Incidencias de Software 2025 e Indicadores Clave de Desempeño (KPIs).	Registros históricos, correos electrónicos, bitácoras operativas, comunicaciones internas y resultados del indicador correspondiente al porcentaje de incidencias gestionadas sin registro formal.
Establecer indicadores de desempeño para evaluar la gestión de incidencias de software del área de Desarrollo en Banco Ficensa.	Matriz Documental de Incidencias de Software 2025 e Indicadores Clave de Desempeño (KPIs).	Registros históricos; tiempos de atención y resolución; formalización del registro; reincidencia; cierre documentado; y métricas definidas para el seguimiento futuro del desempeño del proceso.
Definir un flujo formal de registro, clasificación, escalamiento, seguimiento y cierre de incidencias de software en Banco Ficensa.	Cuestionario de percepción del usuario con escala Likert; Matriz Documental de Incidencias de Software 2025; Matriz de Evaluación de Capacidad del Proceso basada en COBIT 2019; e Indicadores Clave de Desempeño (KPIs).	Datos de percepción sobre el proceso actual; hallazgos documentales; brecha entre el estado actual AS-IS y el estado objetivo TO-BE; métricas requeridas para el seguimiento; y necesidades identificadas para estructurar el flujo formal dentro de la Mesa de Servicio existente.

Fuente: Elaboración Propia

3.7.2.1. CRITERIOS DE CLASIFICACIÓN Y CATEGORIZACIÓN DE INCIDENCIAS

Para la clasificación y análisis de las incidencias de software, se definieron criterios estandarizados de categorización por tipo de incidencia, nivel de criticidad, medio de registro y reincidencia. Estos criterios permitieron estructurar la información obtenida de fuentes

documentales como correos electrónicos, reportes internos y bitácoras operativas, garantizando la consistencia en el registro y el análisis de los datos.

3.7.2.1.1. CLASIFICACIÓN POR TIPO DE INCIDENCIA

Esta clasificación permite categorizar las incidencias según la naturaleza del problema presentado en el sistema, facilitando el análisis de los tipos de fallas más frecuentes y la identificación de patrones en el comportamiento de los sistemas.

Tabla 13: Clasificación por Tipo de Incidencia

Tipo de Incidencia	Descripción	Ejemplo
Falla funcional	El sistema no permite ejecutar una operación esperada	No permite realizar pagos
Error	El sistema presenta mensajes de error o fallas puntuales	Error al generar reporte
Lentitud	El sistema responde de forma lenta	Transacciones tardan en procesar
Caída	El sistema no está disponible	Sistema fuera de línea
Integración	Fallo en comunicación entre sistemas	No conecta con sistema externo
Datos incorrectos	Información generada es errónea	Saldo incorrecto

Fuente: Elaboración Propia.

3.7.2.1.2. CLASIFICACIÓN POR CRITICIDAD

Este criterio establece el nivel de impacto que tiene la incidencia sobre la operación del negocio, permitiendo priorizar su atención en función de la gravedad y urgencia del problema.

Tabla 14: Clasificación por Criticidad

Nivel de Criticidad	Descripción	Impacto Operativo
Alta	Incendencia que detiene operaciones críticas del negocio	No se pueden realizar transacciones o procesos clave
Media	Incendencia que afecta parcialmente la operación	Procesos continúan con limitaciones
Baja	Incendencia con impacto mínimo	No afecta significativamente la operación

Fuente: Elaboración Propia.

3.7.2.1.3. CLASIFICACIÓN POR MEDIO DE REGISTRO

Esta clasificación identifica el canal a través del cual se reporta la incidencia, permitiendo diferenciar entre registros formales y no formales, así como evidenciar la dispersión de los mecanismos de atención.

Tabla 15: Clasificación por Medio de Registro

Medio de Registro	Descripción	Tipo de Registro
Correo electrónico	Reporte enviado por email	Formal
Llamada telefónica	Comunicación verbal vía llamada	No formal
Microsoft Teams/ WhatsApp	Mensajería instantánea	No formal
Verbal	Comunicación directa sin evidencia digital	No formal

Fuente: Elaboración Propia.

3.7.2.1.4. CLASIFICACIÓN POR REINCIDENCIA

Este criterio permite identificar si una incidencia ha ocurrido previamente, facilitando el análisis de recurrencia de fallas y la detección de problemas repetitivos en los sistemas.

Tabla 16: Clasificación por Reincidencia

Clasificación	Descripción
Sí	La incidencia ya ha ocurrido anteriormente en el mismo sistema o proceso
No	Es la primera vez que ocurre la incidencia

Fuente: Elaboración Propia.

3.7.2.1.5. CÁLCULO DE TIEMPOS DE GESTIÓN

Este criterio define la forma en que se calculan los tiempos de atención y resolución de las incidencias, permitiendo establecer una línea base de eficiencia operativa. Los valores obtenidos servirán posteriormente como insumo para definir tiempos objetivo diferenciados según criticidad y evaluar el cumplimiento de acuerdos de nivel de servicio una vez implementado el modelo propuesto.

Tabla 17: Cálculo de Tiempos de Gestión

Indicador	Definición	Fórmula
Tiempo de atención	Tiempo desde el reporte hasta que se inicia la atención	Fecha atención – fecha reporte (días)
Tiempo de resolución	Tiempo desde el reporte hasta la solución	Fecha resolución – fecha reporte(días)

Fuente: Elaboración Propia.

3.7.2.1.6. CLASIFICACIÓN DE REGISTRO FORMAL

Este criterio permite diferenciar las incidencias que cuentan con un registro formal de aquellas gestionadas de manera informal, facilitando la medición del nivel de control y trazabilidad en la gestión de incidencias.

Tabla 18: Clasificación de Registro Formal

Clasificación	Criterio
Formal	Incidencia registrada en correo.
No formal	Incidencia gestionada por llamada, chat o verbal.

Fuente: Elaboración Propia.

3.7.2.2.VALIDACIÓN Y CONFIABILIDAD DEL CUESTIONARIO

El cuestionario de percepción ([Ver Anexo 4](#)) fue sometido a un proceso de validación de contenido mediante juicio experto, previo a su aplicación. La revisión estuvo a cargo del asesor temático de la investigación y de personal de Banco Ficensa con conocimiento directo de la operación y de la gestión de incidencias de software. Este proceso permitió verificar la pertinencia, claridad y suficiencia de los ítems respecto a los objetivos del estudio y a las dimensiones consideradas: tiempos de respuesta y resolución, seguimiento y trazabilidad, efectividad del soporte, satisfacción general y aceptación de una Mesa de Servicio centralizada.

Como resultado de la revisión por juicio experto y de la prueba piloto aplicada a un grupo reducido de colaboradores, se realizaron ajustes al instrumento orientados a mejorar la claridad de la redacción de los ítems y a asegurar su comprensión uniforme por parte de los encuestados, antes del levantamiento definitivo de información.

La confiabilidad del instrumento se evaluó mediante el análisis de consistencia interna de la escala de percepción, aplicando el coeficiente alfa de cronbach sobre las respuestas recolectadas. El análisis, realizado sobre los quince ítems que integran la escala de percepción y satisfacción (ítems detallados en el [Anexo 4](#)), arrojó un valor de $\alpha = 0.807$, considerado bueno según los criterios convencionales de interpretación, que establecen valores superiores a 0.70 como indicativos de una confiabilidad aceptable (Hernández Sampieri y otros, 2014). Este resultado confirma que los ítems miden de manera coherente el constructo de percepción del usuario sobre la gestión actual de incidencias de software.

La escala de percepción se conformó por los quince ítems orientados a valorar la calidad del servicio actual y la disposición hacia un modelo centralizado. Los ítems restantes del cuestionario, de carácter diagnóstico sobre hábitos de reporte y dificultades del proceso, se analizaron de forma descriptiva e independiente en el capítulo IV.

Finalmente, respecto al tratamiento de respuestas incompletas, el cuestionario se

administró mediante un formulario digital con campos de respuesta obligatoria, lo que impidió el envío de formularios parcialmente contestados. En consecuencia, no se registraron datos faltantes y la totalidad de los 110 cuestionarios recolectados resultó válida para el análisis, garantizando la integridad del conjunto de datos.

3.7.3. PROCEDIMIENTOS

En la presente investigación, los procedimientos se desarrollarán con el propósito de recolectar, organizar y analizar información documental y datos cuantitativos de percepción que permitan examinar la situación actual de la gestión de incidencias de software en Banco Ficensa durante el año 2025.

Para evitar ambigüedades metodológicas, se establecerán dos fuentes de información diferenciadas por un lado, los registros documentales de incidencias, utilizados como fuente principal para cuantificar casos, tiempos, canales, criticidad, áreas afectadas y nivel de formalización del registro; y, por otro lado, el cuestionario de percepción, utilizado como fuente complementaria para conocer la experiencia de los usuarios respecto al proceso actual de atención, seguimiento, trazabilidad y aceptación de una Mesa de Servicio centralizada.

En primer lugar, se llevará a cabo el análisis documental de los registros históricos correspondientes al año 2025, utilizando la matriz de recolección de datos documentales definida en la sección anterior. Para ello, se revisarán los diferentes canales de comunicación descentralizados utilizados por los usuarios para reportar incidencias de software, tales como correos electrónicos, registros de llamadas telefónicas y mensajes enviados mediante plataformas de comunicación institucional como Microsoft Teams o WhatsApp.

La información identificada será registrada y categorizada en la matriz documental con el fin de cuantificar el volumen de incidencias de software, clasificar los casos según tipo, criticidad y área afectada, calcular tiempos de atención y resolución, identificar los canales de recepción más utilizados y determinar el porcentaje de incidencias gestionadas sin registro formal.

Posteriormente, se diseñará un cuestionario digital estructurado con escala tipo Likert, cuyo objetivo será medir la percepción de los colaboradores de las áreas de Negocios y Operaciones respecto a la atención de incidencias de software, los tiempos de respuesta y resolución, el seguimiento recibido, la claridad del proceso, la efectividad del soporte técnico, la

satisfacción general y la aceptación de una Mesa de Servicio centralizada.

Este instrumento no tendrá como finalidad sustituir la información documental, sino complementar el diagnóstico mediante la percepción de los usuarios involucrados en el reporte y seguimiento de incidencias.

El cuestionario se administrará de manera individual a través de la plataforma Microsoft Forms. El enlace de participación será enviado mediante correo electrónico corporativo al censo de colaboradores de las áreas de Negocios y Operaciones de Banco Ficensa. Este procedimiento permitirá recopilar datos de forma estructurada, estandarizada y eficiente, garantizando el anonimato y la confidencialidad de las respuestas.

Los datos derivados de la matriz documental y del cuestionario serán organizados en bases de datos independientes. La información documental será tabulada para calcular frecuencias, porcentajes, tiempos promedio, niveles de criticidad, áreas afectadas y proporción de incidencias con o sin registro formal.

Por su parte, las respuestas del cuestionario serán tabuladas para obtener resultados descriptivos sobre la percepción de los usuarios. Ambos conjuntos de información serán consolidados en el análisis, con el propósito de identificar patrones, brechas, tendencias y oportunidades de mejora que sustenten el diseño del modelo formal de gestión de incidencias de software basado en ITIL 4 para Banco Ficensa.

Posteriormente, se aplicó la Matriz de Evaluación de Capacidad del Proceso basada en COBIT 2019. Para ello, se contrastaron los resultados del cuestionario de percepción y de la Matriz Documental de Incidencias de Software con los criterios establecidos para cada nivel de capacidad. Esta evaluación permitió determinar el estado actual AS-IS, el estado objetivo TO-BE y la brecha que deberá atenderse mediante la propuesta. A partir de estos resultados se consolidó la línea base de KPIs y se estructuró la Matriz RA del proceso, utilizada para definir la distribución de responsabilidades dentro del flujo formal.

3.7.4. PLAN DE ANÁLISIS

El plan de análisis establece el procedimiento mediante el cual se procesará, organizará e interpretará la información recopilada durante la investigación, con el propósito de responder a los objetivos planteados y analizar la gestión de incidencias de software en las áreas de Negocios y

Operaciones de Banco Ficensa durante el año 2025.

En esta investigación se empleará un análisis cuantitativo de tipo descriptivo, basado en la organización, clasificación y resumen de los datos obtenidos mediante los instrumentos de recolección de información. Este análisis permitirá identificar el comportamiento de las incidencias de software, los tiempos de atención y resolución, el nivel de formalización del registro, la criticidad de los casos, la reincidencia, el cumplimiento de tiempos esperados y la percepción de los usuarios respecto al proceso actual de atención.

La información obtenida a través de la matriz documental de incidencias de software será sistematizada en una base de datos para su posterior análisis en Power BI. Los registros identificados en correos electrónicos, reportes internos, bitácoras operativas y registros del área de tecnología serán clasificados de acuerdo con los criterios definidos en la operacionalización de variables, considerando dimensiones como registro, clasificación, priorización, formalización del registro, seguimiento y cierre de incidencias. A partir de estos datos se calcularán frecuencias, porcentajes, tiempos promedio y tasas relacionadas con los indicadores establecidos.

Para el análisis de la eficiencia operativa del proceso de atención de incidencias, se calcularán el tiempo promedio de atención, el tiempo promedio de resolución de incidencias (MTTR) y la tasa de reincidencia, tomando como referencia los datos verificables disponibles en los registros documentales del año 2025. Asimismo, se calculará el porcentaje de incidencias gestionadas sin registro formal como indicador del nivel actual de trazabilidad del proceso.

De forma complementaria, se incorporarán dos indicadores para el seguimiento futuro del modelo propuesto: el cumplimiento de acuerdos de nivel de servicio (SLA) y el porcentaje de incidencias con trazabilidad completa. Estos indicadores deberán medirse una vez que las incidencias de software sean integradas formalmente dentro de la Mesa de Servicio institucional y se definan los tiempos objetivo y campos obligatorios de seguimiento.

Los resultados derivados de la matriz documental y del cuestionario de percepción serán integrados para generar una visión global de la situación actual de la gestión de incidencias de software en Banco Ficensa. Los hallazgos serán presentados mediante tablas, gráficos estadísticos y descripciones analíticas, procurando que cada resultado responda directamente a los objetivos específicos de la investigación. Esta integración permitirá sustentar la formulación de indicadores de desempeño y la definición de un flujo formal de registro, clasificación, escalamiento,

seguimiento y cierre de incidencias de software, alineado con las buenas prácticas de ITIL 4.

Con el fin de relacionar los objetivos específicos, las fuentes de información, los instrumentos utilizados, las técnicas de análisis y los resultados esperados, se presenta a continuación la tabla del plan de análisis:

Tabla 19. Plan de Análisis Cuantitativo

Objetivo específico	Fuente de información	Instrumento	Técnica de análisis	Resultado esperado
Analizar la situación actual de la gestión de incidencias de software en las áreas de Negocios y Operaciones de Banco Ficensa durante el año 2025, con base en el registro, la trazabilidad, la frecuencia de ocurrencia y el control operativo de los casos reportados.	Registros históricos de incidencias del año 2025.	Matriz documental de incidencias de software y cuestionario de percepción del usuario con escala Likert.	Tabulación de frecuencias y porcentajes; análisis descriptivo de registros formales e informales; análisis de percepción mediante promedios y distribución de respuestas Likert.	Diagnóstico de la situación actual del proceso de gestión de incidencias, incluyendo frecuencia, formalización del registro, estado de los casos y percepción del usuario sobre el proceso actual.
Calcular el tiempo promedio de atención y resolución de las incidencias de software registradas en el año 2025 en Banco Ficensa.	Registros documentales con fecha/hora de reporte, primera atención y cierre.	Matriz documental de incidencias de software.	Cálculo de diferencias de tiempo y promedios descriptivos.	Tiempo promedio de atención y tiempo promedio de resolución de incidencias (MTTR) para la línea base 2025.
Clasificar y cuantificar las incidencias de software según tipo, criticidad y área afectada durante el año 2025 en Banco Ficensa.	Registros históricos clasificados por tipo, criticidad y área.	Matriz documental de incidencias de software.	Clasificación, conteo, frecuencias absolutas y porcentajes por tipo de incidencia, nivel de criticidad y área afectada.	Distribución cuantitativa de incidencias por tipo, criticidad y área afectada.
Determinar el porcentaje de incidencias de software gestionadas sin registro formal durante el año 2025 en Banco Ficensa.	Registros documentales y evidencia de incidencias atendidas por canales no formales.	Matriz documental de incidencias de software.	Clasificación formal/no formal; conteo de incidencias; cálculo porcentual.	Porcentaje de incidencias gestionadas sin registro formal y nivel de formalización del proceso actual.

Establecer indicadores de desempeño para evaluar la gestión de incidencias de software del área de Desarrollo en Banco Ficensa.	Resultados de la matriz documental, base de SLA y resultados del cuestionario de percepción del usuario.	Matriz documental de incidencias de software y cuestionario de percepción del usuario con escala Likert.	Cálculo de cuatro indicadores de línea base y definición de dos indicadores de seguimiento futuro.	Línea base del proceso mediante el porcentaje de incidencias gestionadas sin registro formal, tiempo promedio de atención, MTTR y tasa de reincidencia; además, definición del cumplimiento de SLA y del porcentaje de incidencias con trazabilidad completa para el seguimiento posterior del modelo.
Definir un flujo formal de registro, clasificación, escalamiento, seguimiento y cierre de incidencias de software en Banco Ficensa.	Hallazgos del análisis documental, resultados de percepción del usuario y criterios derivados de ITIL 4.	Matriz documental de incidencias de software, cuestionario de percepción del usuario y revisión metodológica de ITIL 4.	Análisis de brechas entre el proceso actual y el flujo esperado; síntesis de hallazgos; identificación de etapas requeridas del proceso.	Base diagnóstica para diseñar el flujo formal de gestión de incidencias de software, incluyendo registro, clasificación, priorización, escalamiento, seguimiento y cierre.

Fuente: Elaboración Propia

3.8. FUENTES DE INFORMACIÓN

Para el desarrollo de la presente investigación se utilizarán fuentes de información primarias y secundarias, las cuales permitirán obtener los datos necesarios para el análisis de la gestión de incidencias de software que afectan a las áreas de Negocios y Operaciones del Banco Ficensa.

3.8.1. FUENTES PRIMARIAS

Las fuentes primarias corresponden a la información obtenida directamente de los usuarios y de los registros operativos de la organización. En esta investigación se consideran como fuentes primarias:

- Los registros de incidencias de software, identificados a partir de correos electrónicos, comunicaciones internas y reportes operativos del área de tecnología.
- Las respuestas obtenidas a través del cuestionario estructurado, aplicado a los empleados de las áreas de Negocios y Operaciones del Banco Ficensa, utilizando una escala de Likert para medir la percepción de los usuarios sobre la gestión de incidencias.

Estas fuentes permitirán recopilar información directa relacionada con la frecuencia de las incidencias, los tiempos de atención y resolución, así como la percepción de los usuarios sobre el servicio brindado por el área de tecnología.

3.8.2. FUENTES SECUNDARIAS

Las fuentes secundarias corresponden a información obtenida a partir de documentos, libros, artículos académicos y normativa relacionada con la gestión de servicios de tecnología de la información.

- Entre las principales fuentes secundarias utilizadas en esta investigación se encuentran:
- Literatura especializada sobre gestión de servicios de tecnología de la información.
- Documentación relacionada con las mejores prácticas de gestión de incidencias establecidas en ITIL 4.
- Artículos académicos, investigaciones y publicaciones relacionadas con la gestión de incidentes en organizaciones.

Estas fuentes permitirán sustentar el marco teórico de la investigación y proporcionar el respaldo conceptual necesario para el análisis de los resultados y la elaboración de la propuesta de mejora.

3.9. MATRIZ METODOLÓGICA

Tabla 20: Matriz Metodológica

Preguntas de investigación	Objetivo	Variables	Indicadores	Instrumentos
¿Cuál es la situación actual de la gestión de incidencias de software en las áreas de Negocios y Operaciones de Banco Ficensa durante el año 2025, en términos de registro, trazabilidad, frecuencia de ocurrencia y control operativo	Analizar la situación actual de la gestión de incidencias de software en las áreas de Negocios y Operaciones de Banco Ficensa durante el año 2025, con base en el registro, la trazabilidad, la frecuencia de ocurrencia y el control operativo de los casos reportados.	Gestión de incidencias de software	Frecuencia de incidencias; Porcentaje de incidencias gestionadas sin registro formal; Estado de la incidencia	Matriz documental de incidencias de software

de los casos reportados?				
¿Cuál es el tiempo promedio de atención y resolución de las incidencias de software registradas durante el año 2025 en Banco Ficensa?	Calcular el tiempo promedio de atención y resolución de las incidencias de software registradas en el año 2025 en Banco Ficensa.	Eficiencia operativa del proceso de atención de incidencias	Tiempo promedio de atención; Tiempo promedio de resolución	Matriz documental de incidencias de software
¿Cómo se clasifican y cuál es la distribución cuantitativa de las incidencias de software según tipo, criticidad y área afectada durante el año 2025 en Banco Ficensa?	Clasificar y cuantificar las incidencias de software según tipo, criticidad y área afectada durante el año 2025 en Banco Ficensa.	Gestión de incidencias de software	Tipo de incidencias registradas; Nivel de criticidad de incidencias	Matriz documental de incidencias de software
¿Qué porcentaje de incidencias de software fueron gestionadas sin registro formal durante el año 2025 en Banco Ficensa?	Determinar el porcentaje de incidencias de software gestionadas sin registro formal durante el año 2025 en Banco Ficensa.	Gestión de incidencias de software	Porcentaje de incidencias gestionadas sin registro formal	Matriz documental de incidencias de software
¿Qué indicadores de desempeño deben establecerse para evaluar la gestión de incidencias de software del área de Desarrollo en Banco Ficensa?	Establecer indicadores de desempeño para evaluar la gestión de incidencias de software del área de Desarrollo en Banco Ficensa.	Eficiencia operativa del proceso de atención de incidencias	Línea base 2025: porcentaje de incidencias gestionadas sin registro formal; tiempo promedio de atención; tiempo promedio de resolución de incidencias (MTTR); tasa de reincidencia. Seguimiento futuro: cumplimiento de acuerdos de nivel de servicio (SLA); porcentaje de incidencias con trazabilidad completa.	Matriz documental de incidencias de software y cuestionario de percepción del usuario

¿Cuál debe ser el flujo formal de registro, clasificación, escalamiento, seguimiento y cierre de incidencias de software en Banco Ficensa?	Definir un flujo formal de registro, clasificación, escalamiento, seguimiento y cierre de incidencias de software en Banco Ficensa.	Gestión de incidencias de software	Frecuencia de incidencias; Tipo de incidencias registradas; Nivel de criticidad de incidencias; Estado de la incidencia	Matriz documental de incidencias de software
--	---	------------------------------------	---	--

Fuente: Elaboración Propia

4. CAPÍTULO IV. RESULTADOS Y ANÁLISIS

En este capítulo se presentan los resultados obtenidos a partir del proceso de recolección de datos realizado para analizar la situación actual de la gestión de incidencias de software en Banco Ficensa. La información recopilada permite conocer la forma en que actualmente se reportan, atienden, documentan y dan seguimiento a las incidencias que afectan a las áreas de Negocios y Operaciones.

El análisis se desarrolla con base en los instrumentos definidos en la metodología de la investigación, principalmente el cuestionario de percepción aplicado a los usuarios involucrados y la matriz documental de incidencias de software correspondiente al período de estudio. Estos instrumentos permiten identificar aspectos relevantes como los canales utilizados para reportar incidencias, los tiempos de atención y resolución, la existencia o ausencia de registros formales, la frecuencia de los casos reportados y las principales oportunidades de mejora en el proceso actual.

Los resultados presentados en este capítulo constituyen la base para comprender las debilidades del modelo actual de atención de incidencias y sirven como insumo para el diseño de una propuesta de gestión de incidencias de software basada en ITIL 4, orientada a mejorar la trazabilidad, el control operativo, la priorización y el seguimiento de los casos reportados.

4.1. INFORME DE PROCESO DE RECOLECCIÓN DE DATOS

Para la recolección de datos se aplicó una encuesta al personal de las áreas de Negocios y Operaciones de Banco Ficensa. La población total considerada para el estudio fue de 303 empleados, de los cuales se seleccionó una muestra de 110 colaboradores, a quienes se les aplicó el instrumento de recolección de información.

Asimismo, se utilizó una matriz documental de incidencias de software correspondientes al año 2025, con el propósito de analizar los casos reportados, los canales de atención, los tiempos de gestión, la clasificación de las incidencias y la existencia de registros formales. Esta información permitió complementar los resultados obtenidos mediante la encuesta y obtener una visión más completa sobre la situación actual de la gestión de incidencias de software en Banco Ficensa.

4.2. RESULTADOS Y ANÁLISIS

La encuesta se estructuró en tres secciones principales: información sociodemográfica,

hábitos de reporte actuales y evaluación de percepción y satisfacción. Esta división permite analizar, en primer lugar, las características generales de los participantes; posteriormente, conocer la forma en que actualmente reportan las incidencias de software; y finalmente, evaluar su percepción sobre la atención recibida, los tiempos de respuesta, el seguimiento de los casos y la necesidad de fortalecer el proceso actual.

Asimismo, se integra el análisis de la matriz documental de incidencias de software correspondiente al año 2025, con el propósito de complementar los resultados obtenidos mediante la encuesta y obtener una visión más clara sobre los canales de reporte, tiempos de atención, tiempos de resolución, clasificación de incidencias y existencia de registros formales.



Figura 18. Relación de objetivos con instrumentos.

Fuente: Elaboración propia

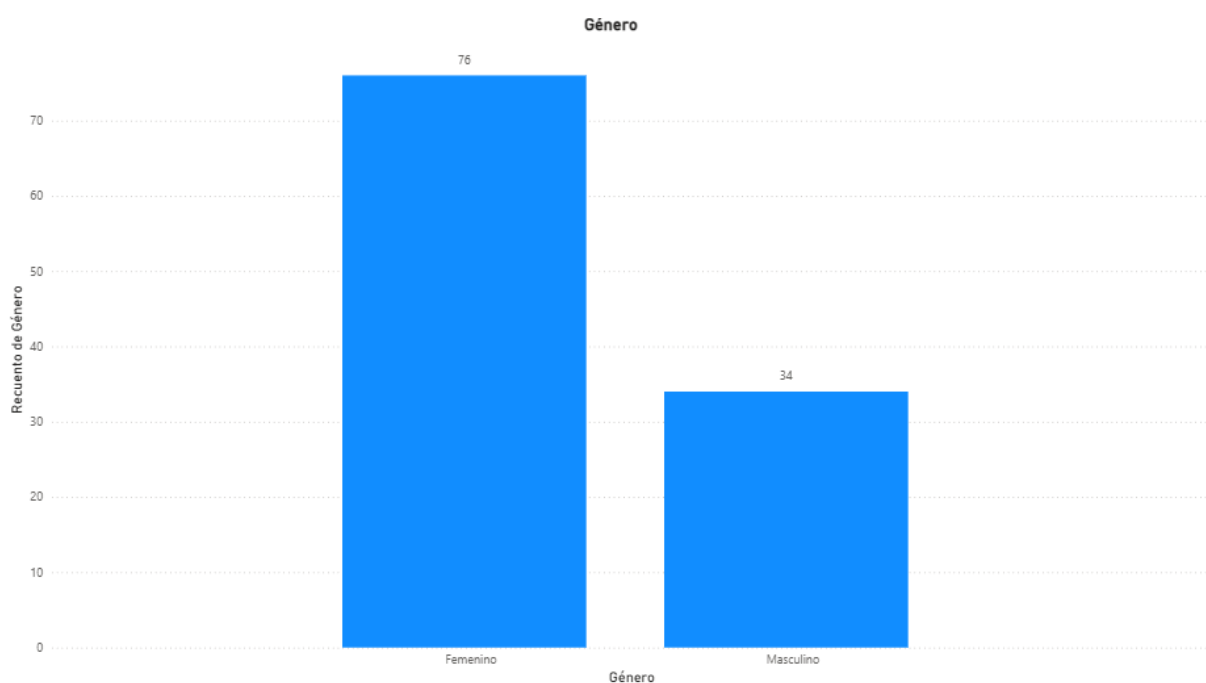
4.2.1. ANÁLISIS CUESTIONARIO DE PERCEPCIÓN DE USUARIOS DE BANCO FICENSA

En este apartado se analizan los resultados del cuestionario aplicado a 110 colaboradores vinculados principalmente con las áreas de Negocios y Operaciones de Banco Ficensa. El propósito no se limita a describir porcentajes, sino a identificar cómo las prácticas actuales de reporte, seguimiento y resolución de incidencias de software influyen en la trazabilidad, la

continuidad de los procesos y la percepción del servicio brindado por TI. La interpretación se organiza en tres dimensiones: caracterización de la muestra, hábitos de reporte y valoración de la atención recibida. Los resultados se contrastan con el marco de ITIL 4 y con investigaciones previas sobre mesas de servicio, formalización de incidentes y mejora de la gestión ITSM, con el fin de contextualizar las brechas identificadas y sustentar la propuesta de un modelo institucional.

4.2.1.1.SECCIÓN I. INFORMACIÓN SOCIODEMOGRÁFICA

Gráfico 1: Género



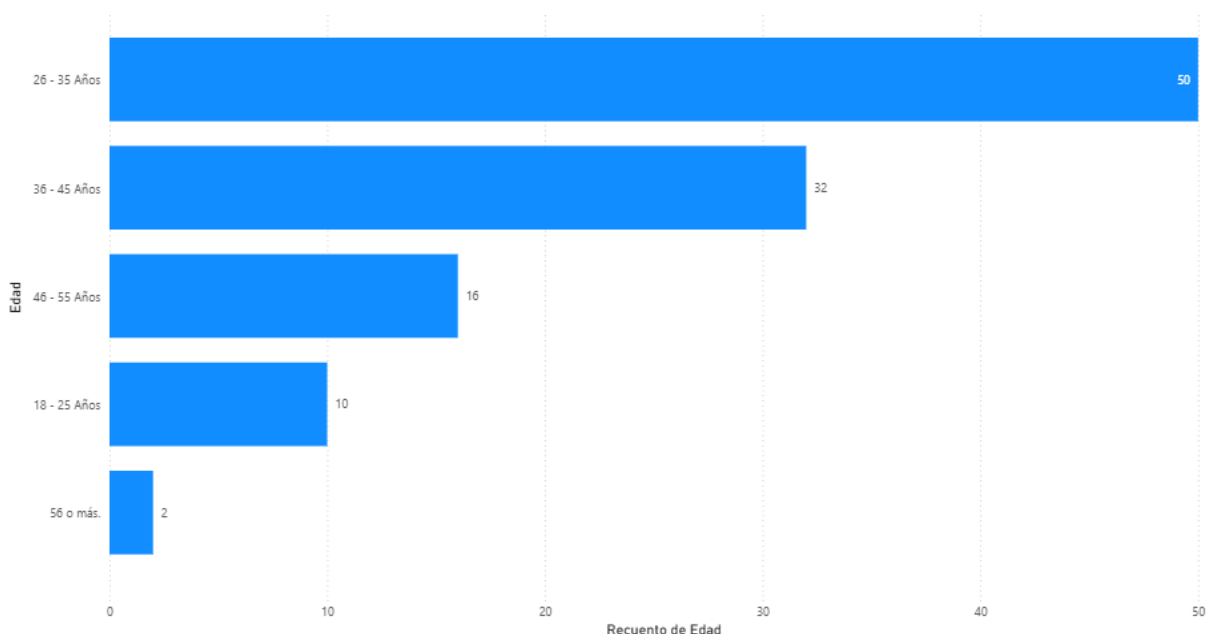
Fuente: Elaboración Propia.

De los 110 colaboradores encuestados, 76 corresponden al género femenino, equivalente al 69.09% de la muestra, mientras que 34 corresponden al género masculino, equivalente al 30.91%. La distribución muestra una participación mayoritaria de colaboradoras, aunque ambos grupos se encuentran representados dentro del levantamiento de información.

Este dato sirve para describir quiénes participaron en la consulta. No permite explicar por sí mismo las fallas del proceso de atención, pero sí confirma que el diagnóstico recoge la opinión de distintos usuarios internos que trabajan con los sistemas del banco. Por esa razón, los gráficos siguientes deben leerse como una valoración general del servicio y no como la experiencia de un único grupo.

La composición de la muestra resulta adecuada para contextualizar el estudio. En este caso no corresponde formular conclusiones causales a partir del género; el foco debe mantenerse en la forma en que se registran, atienden y dan seguimiento a las incidencias de software.

Gráfico 2: Edad



Fuente: Elaboración Propia.

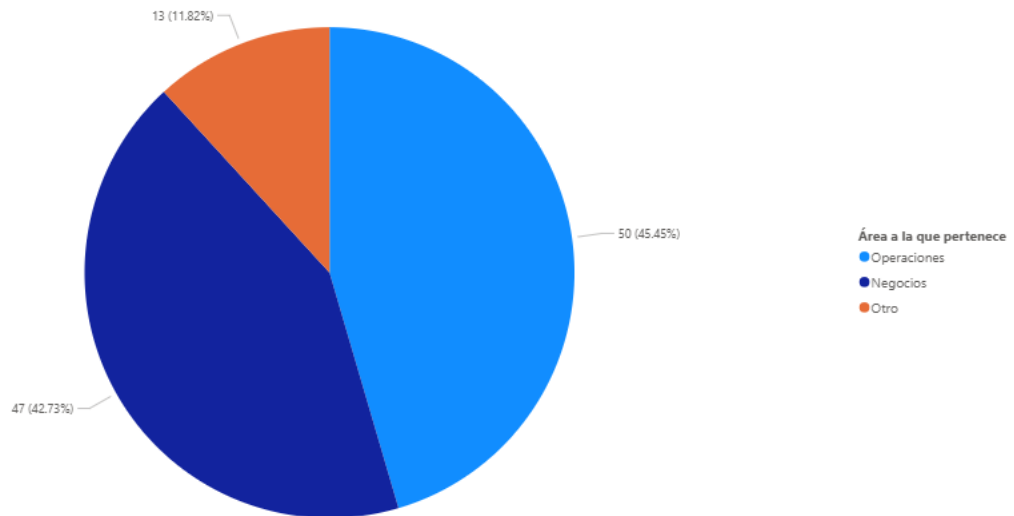
El rango de edad con mayor representación es el de 26 a 35 años, con 50 participantes, equivalente al 45.45% de la muestra. Le siguen los colaboradores de 36 a 45 años, con 32 respuestas (29.09%); de 46 a 55 años, con 16 respuestas (14.55%); de 18 a 25 años, con 10 respuestas (9.09%); y de 56 años o más, con 2 respuestas (1.82%). En conjunto, el 74.54% de los encuestados se concentra entre los 26 y 45 años.

La mayor parte de las respuestas proviene de colaboradores que se encuentran en rangos de edad con alta participación en la operación diaria. Esto favorece el diagnóstico, ya que se trata de usuarios que interactúan de manera frecuente con las aplicaciones utilizadas por Negocios y Operaciones. Aun así, no sería correcto atribuir la aceptación de un canal formal únicamente a la edad. La facilidad de uso, la comunicación interna y la claridad del procedimiento también influyen.

La incorporación futura Mesa de Servicio debería ser sencilla de utilizar para cualquier colaborador, independientemente de su perfil. Este criterio coincide con el principio de ITIL 4 de

mantener los procesos simples y prácticos, de modo que el registro formal ayude al usuario en lugar de convertirse en una carga adicional.

Gráfico 3: Área a la que pertenece



Fuente: Elaboración Propia.

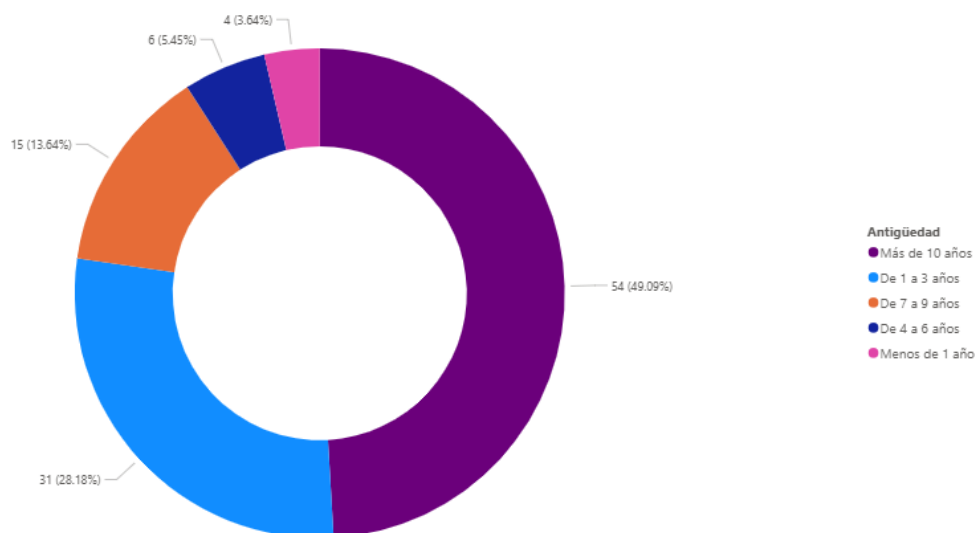
El área de Operaciones registra la mayor participación, con 50 respuestas, equivalente al 45.45% de la muestra. El área de Negocios aporta 47 respuestas, equivalentes al 42.73%, mientras que 13 participantes, equivalentes al 11.82%, pertenecen a otras áreas quienes fueron tomados en esta encuesta ya que usan herramientas de software regulatorias y reportan incidencias de software. En conjunto, Negocios y Operaciones representan el 88.18% de los encuestados.

La distribución es consistente con el alcance de la investigación, porque Negocios y Operaciones concentran la mayoría de las respuestas y dependen directamente de aplicaciones que sostienen actividades comerciales y operativas. Cuando una falla no se resuelve a tiempo, pueden aparecer atrasos, reprocesos y acumulación de tareas. En una institución financiera, estas situaciones también pueden aumentar el riesgo operativo si el personal debe recurrir a controles manuales o coordinaciones improvisadas.

La encuesta recoge principalmente la experiencia de las áreas más expuestas al problema estudiado. Esto permite relacionar las percepciones de los usuarios con la necesidad de fortalecer la continuidad, la trazabilidad y el control operativo, aspectos especialmente importantes en el

sector financiero y coherentes con el enfoque de riesgo operativo.

Gráfico 4: Antigüedad en Banco Ficensa



Fuente: Elaboración Propia.

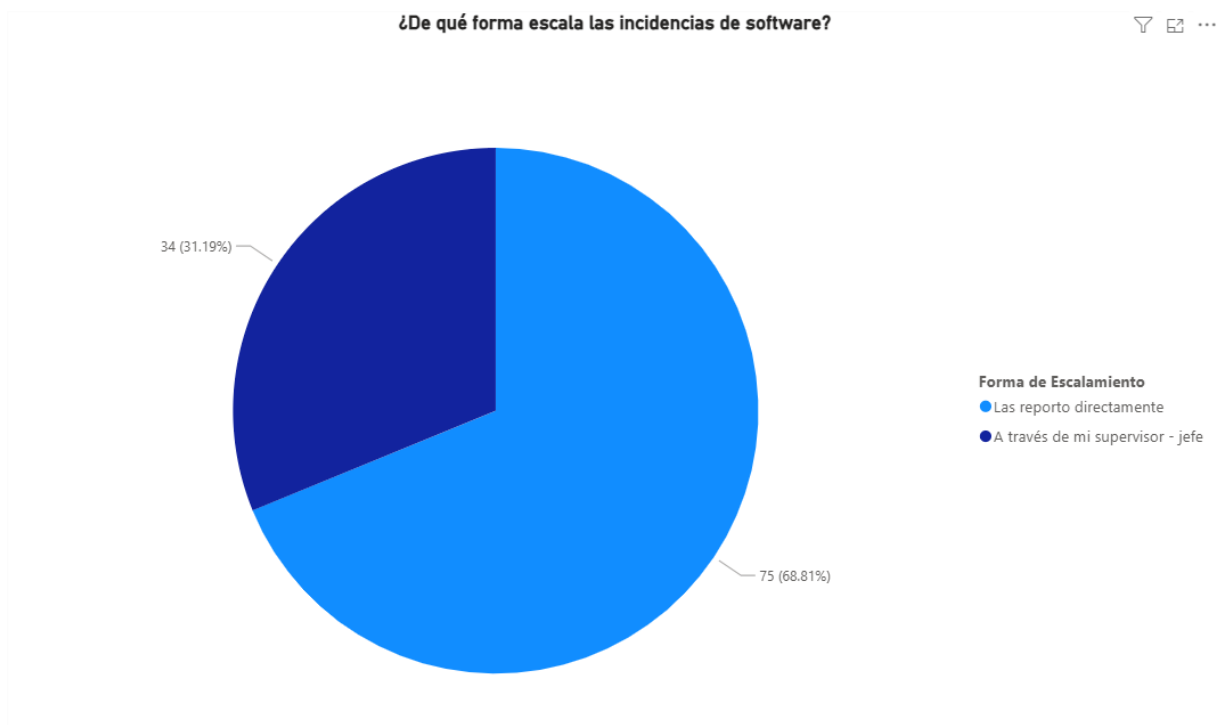
El grupo con mayor representación corresponde a los colaboradores con más de 10 años de antigüedad, con 54 respuestas, equivalente al 49.09% de la muestra. Le siguen quienes tienen entre 1 y 3 años, con 31 respuestas (28.18%); entre 7 y 9 años, con 15 respuestas (13.64%); entre 4 y 6 años, con 6 respuestas (5.45%); y menos de un año, con 4 respuestas (3.64%).

La muestra combina dos perspectivas útiles. Los colaboradores con más años en la institución conocen prácticas que se han vuelto habituales con el tiempo, mientras que quienes ingresaron recientemente pueden notar con mayor facilidad la falta de un canal único o de una confirmación formal. Una gestión basada en contactos directos puede funcionar para quienes ya saben a quién acudir, pero suele ser menos clara para los usuarios nuevos.

La incorporación de un flujo formal en la Mesa de Servicio no debería reducirse a habilitar un ticket. También es requiere comunicar el nuevo procedimiento, capacitar a los usuarios y acompañar el cambio de hábitos, ya que una implementación basada en ITIL depende de factores organizacionales y no solo de la adopción técnica del marco.

4.2.1.2.SECCIÓN II. HÁBITOS DE REPORTE ACTUALES

Gráfico 5. ¿De qué forma escala las incidencias de software?



Fuente: Elaboración Propia.

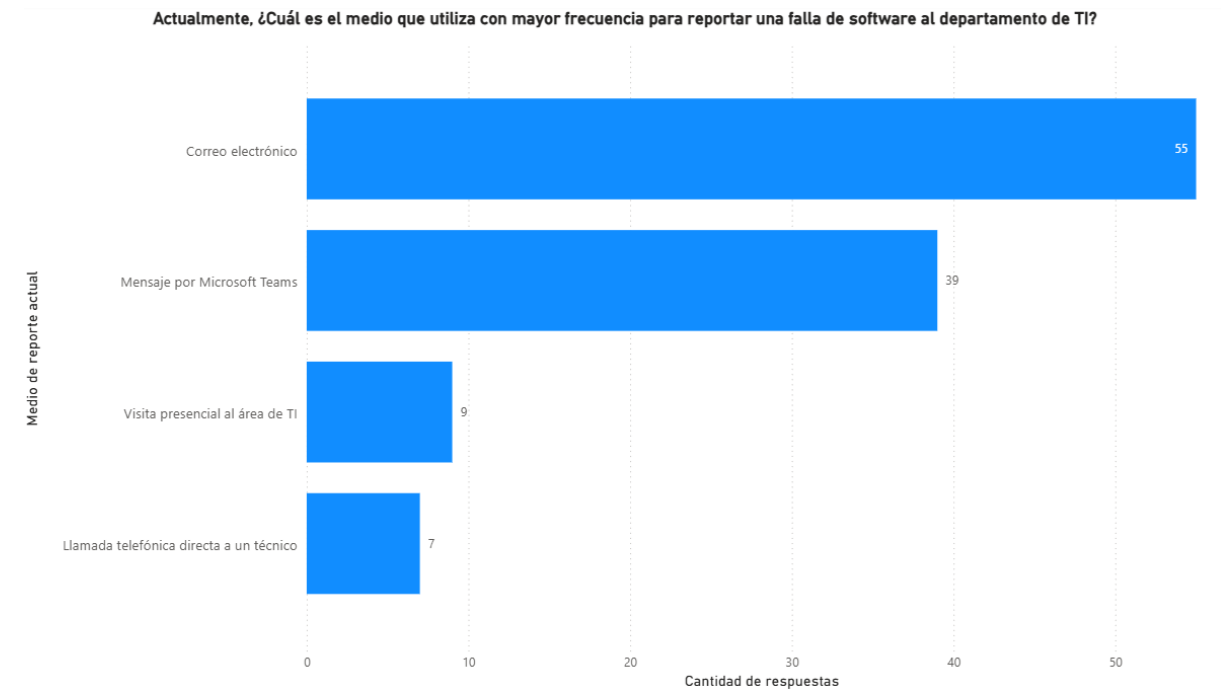
De acuerdo con los resultados obtenidos, el 69.09% de los encuestados indicó que reporta directamente las incidencias de software al área correspondiente, mientras que el 30.91% señaló que realiza el escalamiento a través de su supervisor o jefe inmediato. Esto muestra que la mayoría de los usuarios mantiene una comunicación directa cuando se presenta una falla, aunque todavía existe un grupo considerable que depende de una intermediación jerárquica para canalizar el reporte.

La participación del supervisor o jefe inmediato puede responder a prácticas internas adoptadas por algunas áreas, especialmente cuando el usuario no tiene claridad sobre el canal adecuado, considera que el problema debe ser validado previamente o busca asegurar que la incidencia reciba atención. Sin embargo, esta forma de escalamiento puede generar retrasos desde el momento en que ocurre la falla hasta que el área de TI recibe la información. Además, cuando el reporte pasa por varias personas, existe el riesgo de que los detalles técnicos, el impacto real o el nivel de urgencia no se comuniquen con suficiente precisión.

El resultado refleja la necesidad de establecer un mecanismo formal de reporte que pueda ser utilizado directamente por los usuarios, sin eliminar la posibilidad de que los responsables de

cada área den seguimiento a los casos que afectan procesos relevantes. La implementación de una flujo forma centralizada en una Mesa de Servicio permitiría registrar la incidencia desde su origen, documentar quién la reportó, identificar el área afectada y conservar un historial completo del seguimiento realizado.

Gráfico 6: Actualmente, ¿Cuál es el medio que utiliza con mayor frecuencia para reportar una falla de software al departamento de TI?



Fuente: Elaboración Propia.

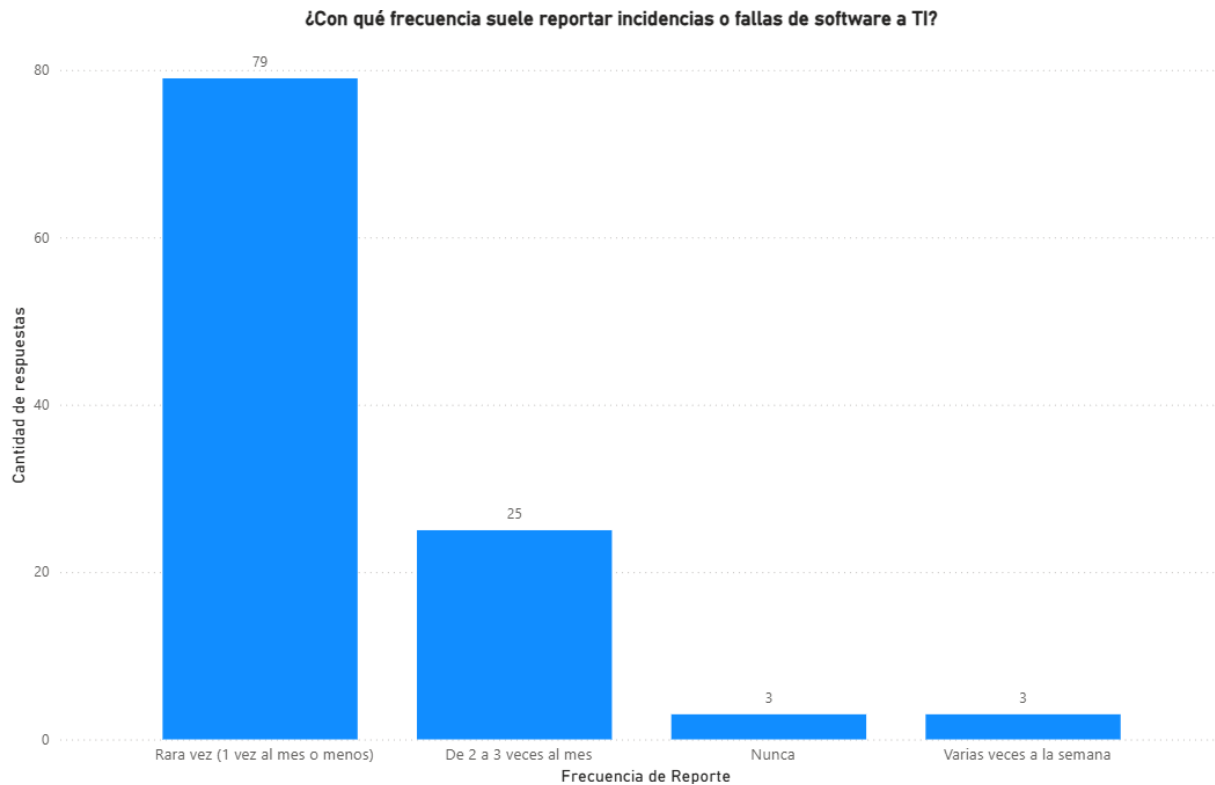
El correo electrónico es el medio más utilizado para reportar fallas de software, con 55 respuestas, equivalente al 50.00% de la muestra. Microsoft Teams ocupa el segundo lugar, con 39 respuestas (35.45%). En menor proporción se utilizan la visita presencial al área de TI, con 9 respuestas (8.18%), y la llamada telefónica directa a un técnico, con 7 respuestas (6.36%).

El correo y Teams facilitan el contacto rápido, pero siguen siendo medios de comunicación y no sustituyen un sistema de gestión. Un mensaje enviado por cualquiera de estos canales no garantiza por sí solo un número de caso, una categoría uniforme, una persona responsable o un historial de estados. En la práctica, esto puede causar pérdida de información, duplicidad de esfuerzos y dificultades para medir con precisión cuánto tarda cada atención.

La comunicación con TI existe, pero no siempre se transforma en un registro trazable. Esa es la brecha central que debe corregirse. La falta de procesos estructurados afecta los informes

de resolución y el control del servicio.

Gráfico 7: ¿Con qué frecuencia suele reportar incidencias o fallas de software a TI?



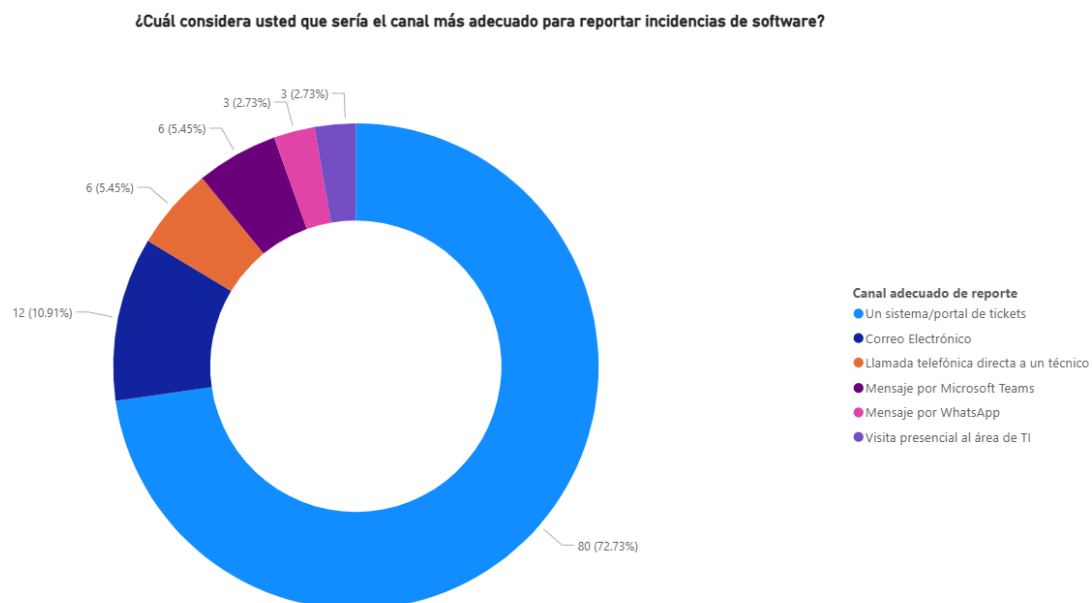
Fuente: Elaboración Propia.

Un total de 79 colaboradores, equivalente al 71.82% de la muestra, indicó que reporta incidencias rara vez, es decir, una vez al mes o menos. Por su parte, 25 participantes (22.73%) reportan de 2 a 3 veces al mes; 3 colaboradores (2.73%) señalaron que nunca reportan incidencias; y otros 3 (2.73%) indicaron que lo hacen varias veces a la semana.

La frecuencia declarada debe revisarse con cuidado. Que la mayoría reporte una vez al mes o menos no significa necesariamente que ocurran pocas fallas. Algunas pueden resolverse entre compañeros, comunicarse por vías informales o simplemente no registrarse cuando el usuario considera que el problema es menor. Si no existe una fuente única, el área de Desarrollo trabaja con una visión parcial de la demanda real.

Este resultado cobra más sentido al compararlo con el Gráfico 12, donde se observa que una parte importante de los usuarios ha resuelto fallas sin reportarlas formalmente. La combinación de ambas respuestas sugiere que la línea base documental podría subestimar el volumen real de incidencias y, por tanto, limitar la planificación de recursos.

Gráfico 8: ¿Cuál considera usted que sería el canal más adecuado para reportar incidencias de software?



Fuente: Elaboración Propia.

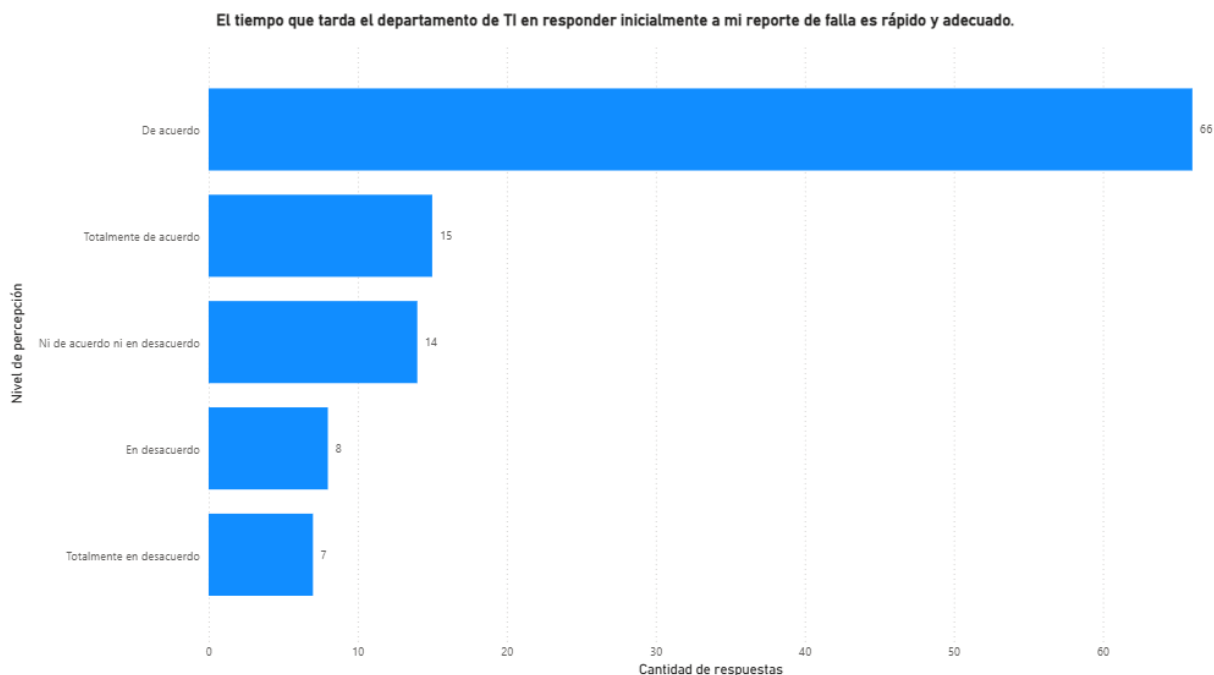
El sistema o portal de tickets es el canal preferido por 80 colaboradores, equivalente al 72.73% de la muestra. El correo electrónico ocupa el segundo lugar, con 12 respuestas (10.91%). La llamada telefónica directa a un técnico y Microsoft Teams registran 6 respuestas cada uno (5.45% respectivamente), mientras que WhatsApp y la visita presencial al área de TI obtienen 3 respuestas cada uno (2.73% respectivamente).

La preferencia por un sistema de tickets muestra que los usuarios perciben la utilidad de un canal único. Un sistema de este tipo permitiría registrar fechas, clasificar el impacto, asignar responsables y consultar el estado del caso sin depender de mensajes separados. Además de mejorar la experiencia del usuario, ayudaría al banco a conservar evidencia para analizar tendencias y demostrar control.

Existe una base favorable para implementar un flujo formal Mesa de Servicio centralizada, ya que cumple una función crítica en una implementación ITSM, siendo la formalización basada en ITIL 4 mejora la organización del soporte. En Banco Ficensa, el reto consiste en aprovechar esa aceptación y traducirla en un proceso sencillo y consistente.

4.2.1.3. SECCIÓN III. EVALUACIÓN DE PERCEPCIÓN Y SATISFACCIÓN

Gráfico 9: El tiempo que tarda el departamento de TI en responder inicialmente a mi reporte de falla es rápido y adecuado.



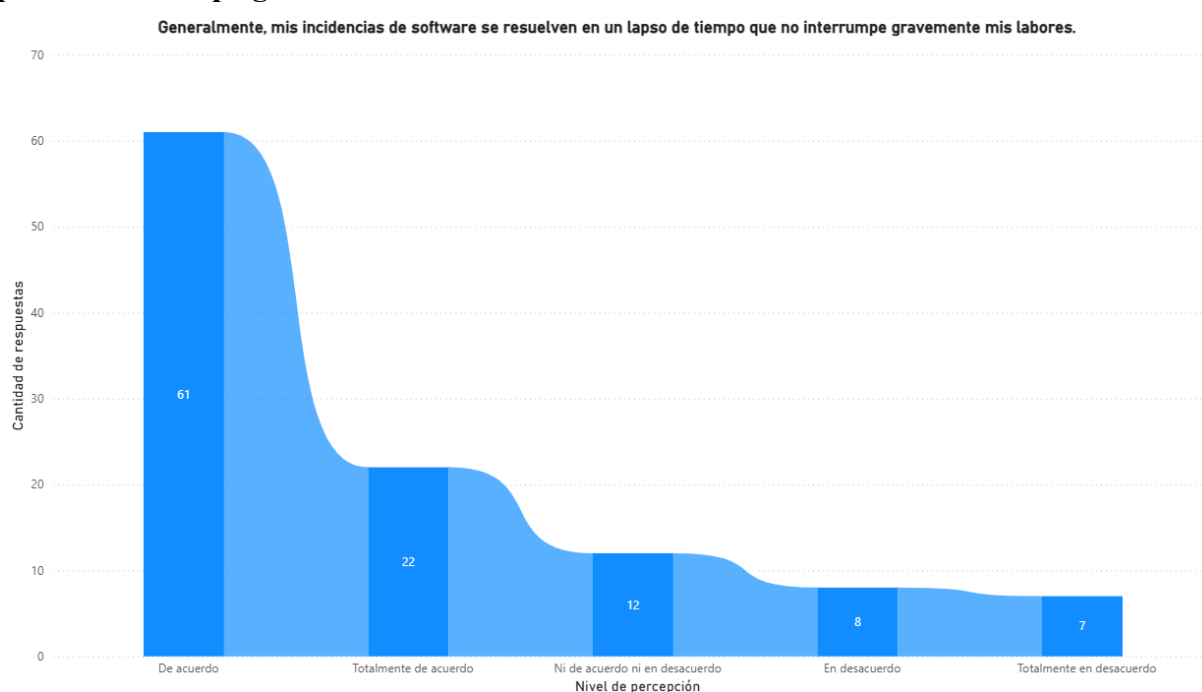
Fuente: Elaboración Propia.

Un total de 81 colaboradores manifestó una percepción favorable sobre el tiempo de respuesta inicial: 66 indicaron estar de acuerdo y 15 totalmente de acuerdo, equivalentes en conjunto al 73.64% de la muestra. Además, 14 participantes (12.73%) se mantuvieron neutrales, mientras que 15 (13.64%) expresaron una percepción desfavorable.

Desde una lectura operativa, el dato podría interpretarse como una fortaleza del proceso actual; sin embargo, desde una visión de negocio bancario, la primera respuesta no solo representa rapidez, sino capacidad de contención temprana. AXELOS (2019) explica que la gestión de incidencias busca reducir el impacto de las interrupciones y restablecer el servicio en el menor tiempo posible. Aplicado a Banco Ficensa, esto significa que una respuesta inicial oportuna permite ordenar la atención, disminuir la incertidumbre del usuario y evitar que el caso escale por canales informales. En un banco, esa primera reacción también ayuda a proteger procesos que dependen de sistemas transaccionales, reportes y atención continua al cliente interno. Este punto coincide con Castro Martínez y Gómez Hernández (2018), quienes advierten en el caso BAC Credomatic que cumplir un SLA o atender un ticket dentro de tiempo no necesariamente significa que la solución haya sido adecuada para el usuario final.

Aunque la percepción general es favorable, el banco no debería depender únicamente de la opinión del usuario para evaluar este punto. El hallazgo estratégico es que se necesita medir formalmente el tiempo de primera respuesta por nivel de criticidad, porque una respuesta inicial rápida, cuando está documentada, permite priorizar mejor, controlar el riesgo operativo y generar evidencia para la toma de decisiones. Este enfoque coincide con COBIT 2019, donde la entrega de servicios de TI debe vincularse con necesidades del negocio, objetivos de control y desempeño institucional (ISACA, 2018).

Gráfico 10: Generalmente, mis incidencias de software se resuelven en un lapso de tiempo que no interrumpe gravemente mis labores.



Fuente: Elaboración Propia.

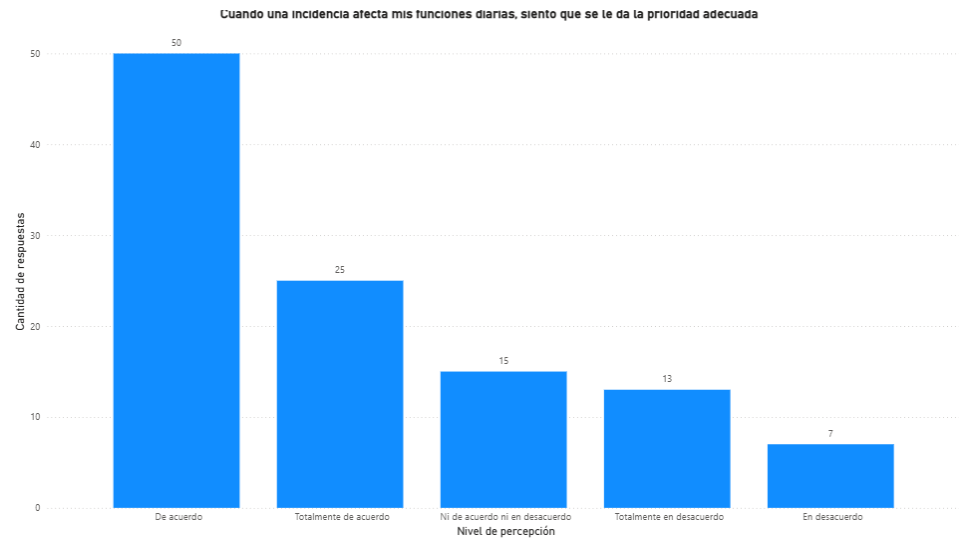
Un total de 83 participantes expresó una valoración favorable: 61 indicaron estar de acuerdo y 22 totalmente de acuerdo, equivalentes al 75.45% de la muestra. Asimismo, 12 colaboradores (10.91%) se mantuvieron neutrales y 15 (13.64%) manifestaron una valoración desfavorable.

Aunque el resultado es positivo no elimina la necesidad de fortalecer el análisis desde el impacto al negocio. En una institución bancaria, una incidencia que tarda en resolverse puede detener procesos de atención, conciliación, aprobación o reporte, generando costos indirectos por reprocesos, horas improductivas y dependencia de soluciones manuales. La Organización

Internacional de Normalización (2019), desde el enfoque de continuidad del negocio, permite comprender que la recuperación oportuna de servicios críticos no es únicamente un asunto técnico, sino una condición para sostener operaciones esenciales. Por ello, el tiempo de resolución debe analizarse como un indicador de continuidad operativa y no solo como una medición de soporte. En una investigación aplicada al sector bancario, Almendarez Rodríguez y Cuellar Varela (2024) plantean que la gestión efectiva de incidentes y solicitudes es crucial para la continuidad operativa y la satisfacción del cliente interno, especialmente cuando la herramienta de mesa de servicio no se encuentra alineada con ITIL V.4.

La satisfacción agregada no es suficiente para evaluar el desempeño. El banco necesita tiempos objetivo según criticidad, reglas de escalamiento y revisión de los casos que excedan esos plazos. Esta orientación es consistente con (AXELOS, 2019), que plantea restablecer el servicio normal lo antes posible para reducir el impacto negativo sobre la operación.

Gráfico 11: Cuando una incidencia afecta mis funciones diarias, siento que se le da la prioridad adecuada.



Fuente: Elaboración Propia.

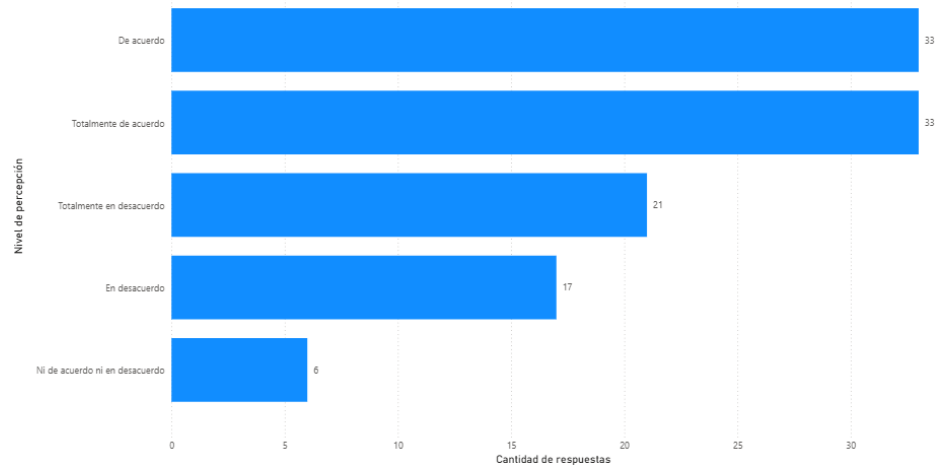
Un total de 75 colaboradores manifestó una percepción favorable sobre la prioridad asignada a las incidencias que afectan sus labores: 50 indicaron estar de acuerdo y 25 totalmente de acuerdo, equivalentes al 68.18% de la muestra. Por otra parte, 15 participantes (13.64%) se mantuvieron neutrales y 20 (18.18%) expresaron una valoración desfavorable.

Este resultado debe analizarse más allá de la satisfacción del usuario. La priorización de

incidencias en un banco no puede depender únicamente de quién reporta, del canal utilizado o de la presión del momento; debe responder a criterios de impacto, urgencia, continuidad operativa, afectación de usuarios y posible exposición regulatoria. En este sentido, COBIT 2019 enfatiza la necesidad de gestionar TI con base en objetivos de gobierno, riesgo y desempeño (ISACA, 2018). Por tanto, la criticidad debe conectarse con procesos del negocio y no únicamente con la dificultad técnica del caso. En el caso de Banco Davivienda, Almendarez Rodríguez y Cuellar Varela (2024) identificaron que la falta de un sistema estructurado de priorización y clasificación era una de las deficiencias que afectaba la calidad de las soluciones y los tiempos de respuesta.

El hallazgo estratégico es que la percepción favorable no garantiza una priorización homogénea. La propuesta debe incorporar una matriz de impacto y urgencia que permita clasificar los casos con criterios comunes. Esto contribuiría a reducir discrecionalidad, mejorar la asignación de recursos y justificar por qué determinadas incidencias deben atenderse antes que otras. En el contexto financiero, este control también fortalece la trazabilidad exigida para gestionar riesgos tecnológicos y continuidad de servicios. (Comisión Nacional de Bancos y Seguros, 2022).

Gráfico 12: En alguna ocasión he resuelto una falla de software por mis propios medios o con apoyo de un compañero, sin reportarla formalmente a TI.



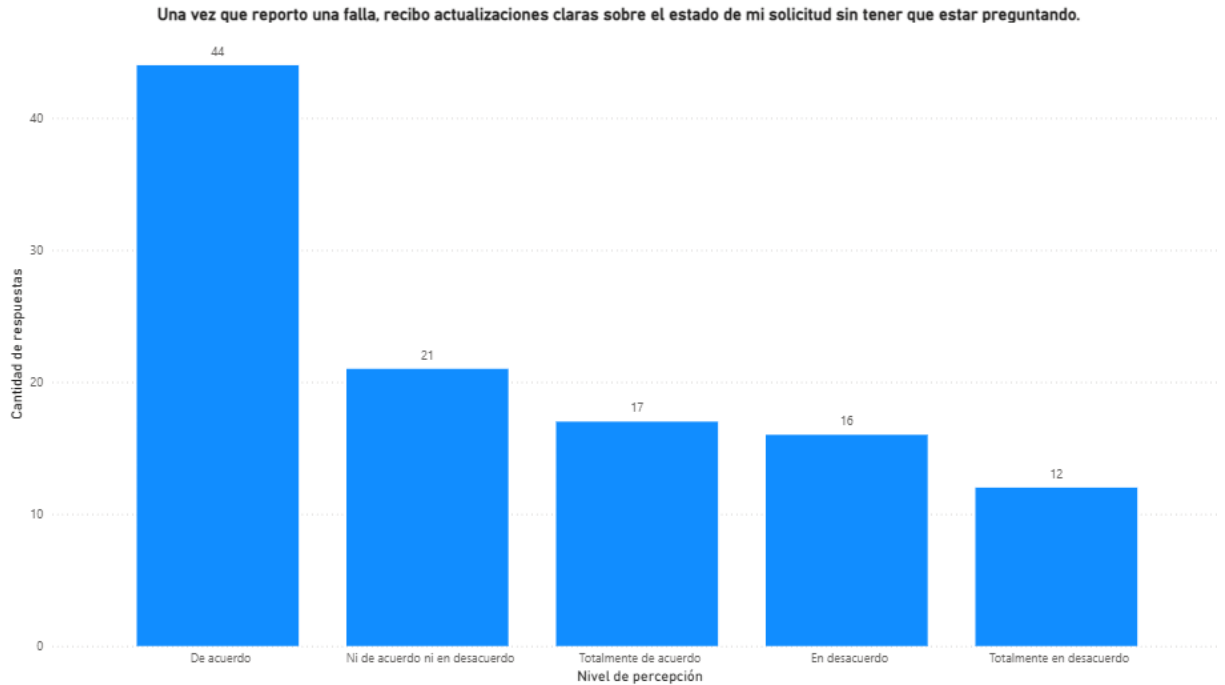
Fuente: Elaboración Propia.

Un total de 66 participantes, equivalente al 60.00% de la muestra, confirmó que en alguna ocasión resolvió una falla de software por sus propios medios o con apoyo de un compañero sin reportarla formalmente a TI. De ellos, 33 indicaron estar de acuerdo y 33 totalmente de acuerdo. Además, 6 colaboradores (5.45%) se mantuvieron neutrales y 38 (34.55%) expresaron desacuerdo.

Este es uno de los resultados más importantes de la encuesta. Resolver una falla con apoyo de un compañero puede ser práctico en el momento, sobre todo cuando el problema parece sencillo o cuando el usuario necesita continuar trabajando. Sin embargo, si el caso no se registra, el banco pierde información sobre la frecuencia de la falla, el sistema afectado y la solución utilizada. Con el tiempo, esto dificulta reconocer patrones y puede ocultar problemas recurrentes.

Los registros disponibles probablemente no reflejan todo lo que ocurre en la operación. Por ello, el modelo debería permitir documentar también las fallas resueltas mediante autoservicio o apoyo interno. El autoservicio solo funciona de manera sostenible cuando se articula con la gestión y la organización.

Gráfico 13: Una vez que reporto una falla, recibo actualizaciones claras sobre el estado de mi solicitud sin tener que estar preguntando.



Fuente: Elaboración Propia.

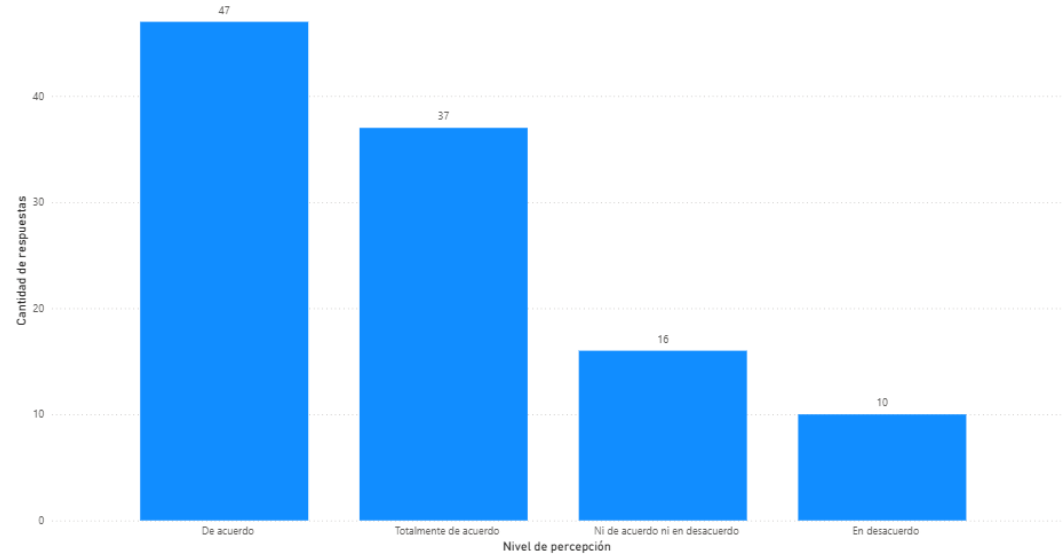
Un total de 61 colaboradores expresó una percepción favorable: 44 indicaron estar de acuerdo y 17 totalmente de acuerdo, equivalentes al 55.45% de la muestra. Por otra parte, 21 participantes (19.09%) se mantuvieron neutrales y 28 (25.45%) manifestaron una valoración desfavorable.

Este resultado evidencia una brecha importante en la experiencia del usuario. Cuando el colaborador no recibe actualizaciones claras, tiende a consultar nuevamente por correo, Teams,

WhatsApp o llamadas, lo que genera duplicidad de esfuerzos y consumo adicional de tiempo. Ayala Soto y Caso Rojas (2023) encontraron que la aplicación de buenas prácticas ITIL en Service Desk puede mejorar la organización de la atención y la satisfacción de los usuarios. En el caso de Banco Ficensa, el seguimiento visible no solo mejora la percepción del servicio, sino que reduce reprocesos y fortalece la transparencia sobre el estado de cada incidencia. De forma similar, Castro Martínez y Gómez Hernández (2018) evidenciaron que la percepción de los colaboradores sobre la atención de tickets no puede evaluarse solo con tiempos de SLA, porque el usuario también valora la comunicación, el seguimiento y la calidad de la solución recibida.

La trazabilidad debe ser visible también para quien reporta. es que el seguimiento no debe depender de que el usuario pregunte. Un flujo formal debe notificar recepción, asignación, avances, cambios de estado, resolución y cierre. Esto fortalece la experiencia del usuario interno, reduce reprocesos y permite que el área de TI demuestre control del ciclo de vida de cada incidencia, en coherencia con los principios de gestión de servicios y mejora continua de ISO/IEC 20000-1 (Organización Internacional de Normalización, 2018).

Gráfico 14: Tengo claro cuál es el canal correcto para reportar una incidencia de software.



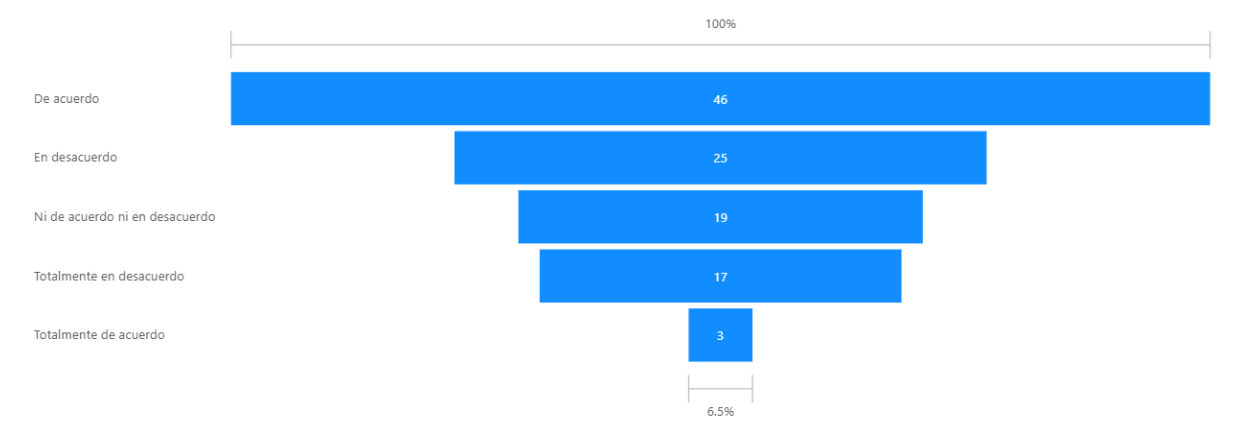
Fuente: Elaboración Propia.

Un total de 84 colaboradores manifestó tener claridad sobre el canal correcto para reportar una incidencia de software: 47 indicaron estar de acuerdo y 37 totalmente de acuerdo, equivalentes al 76.36% de la muestra. Además, 16 participantes (14.55%) se mantuvieron neutrales y 10 (9.09%) expresaron desacuerdo.

Aunque la mayoría afirma conocer el canal correcto, el resultado debe interpretarse junto con la realidad actual: se utilizan correo, Teams, llamadas y visitas presenciales. Es posible que distintas personas consideren oficial un medio diferente. En ese caso, existe claridad individual, pero no necesariamente una regla institucional compartida. La consecuencia es que la calidad del registro puede variar según el canal elegido.

Conviene diferenciar entre saber cómo contactar a TI y disponer de un canal único para gestionar incidencias. El banco debería comunicar con claridad cuál es el medio oficial y establecer una regla simple: cualquier solicitud recibida por otra vía debe convertirse en un ticket para conservar el control y la medición.

Gráfico 15: En ocasiones he tenido dudas sobre si mi incidencia fue realmente registrada o tomada en cuenta.



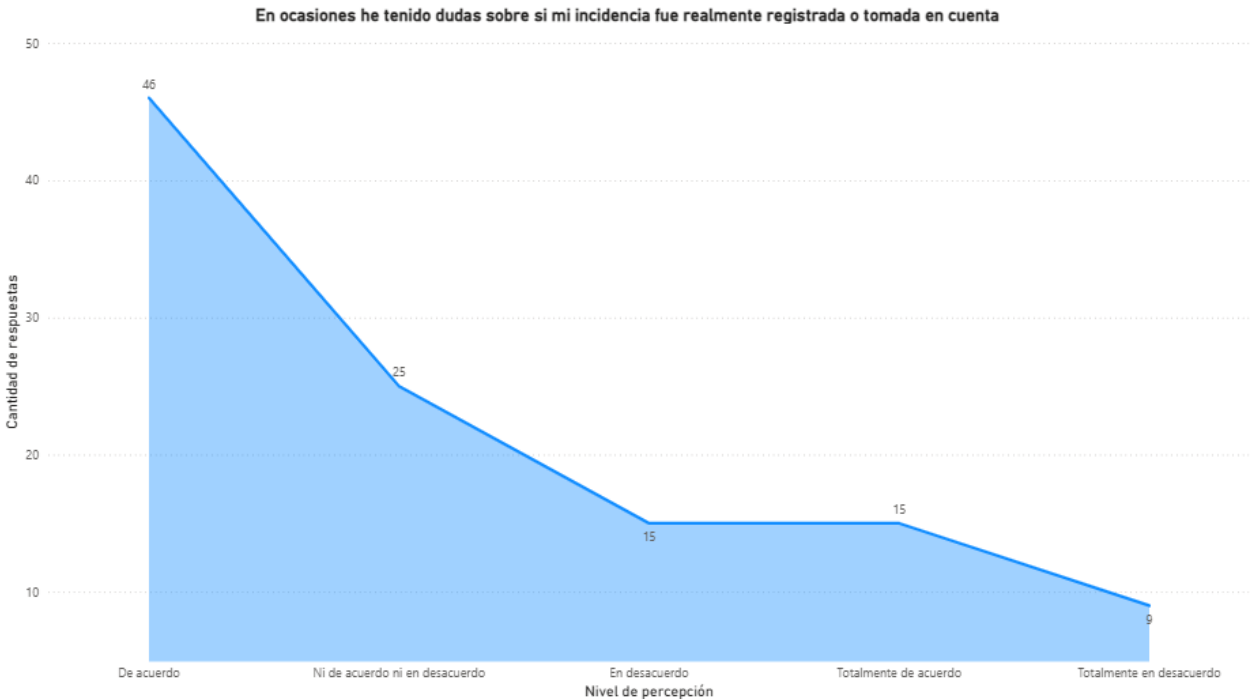
Fuente: Elaboración Propia.

Un total de 49 colaboradores indicó haber tenido dudas sobre si su incidencia fue realmente registrada o tomada en cuenta: 46 respondieron estar de acuerdo y 3 totalmente de acuerdo, equivalentes al 44.55% de la muestra. Asimismo, 19 participantes (17.27%) se mantuvieron neutrales y 42 (38.18%) manifestaron desacuerdo.

Las respuestas reflejan una experiencia dividida. Casi la mitad de los usuarios ha dudado en algún momento si su caso realmente quedó registrado. Esto suele ocurrir cuando no se entrega un número de ticket, una confirmación automática o una forma sencilla de consultar el estado. La incertidumbre termina generando reenvíos, consultas por diferentes medios y tiempo adicional para usuarios y técnicos.

Una confirmación de recepción es un control básico que no debería faltar. El nuevo modelo debe asignar un identificador único, registrar la fecha y mostrar un estado inicial. Con ello se mejora la confianza del usuario y se crea evidencia desde el primer contacto.

Gráfico 16: La falta de un canal único dificulta dar seguimiento a las incidencias que he reportado.



Fuente: Elaboración Propia.

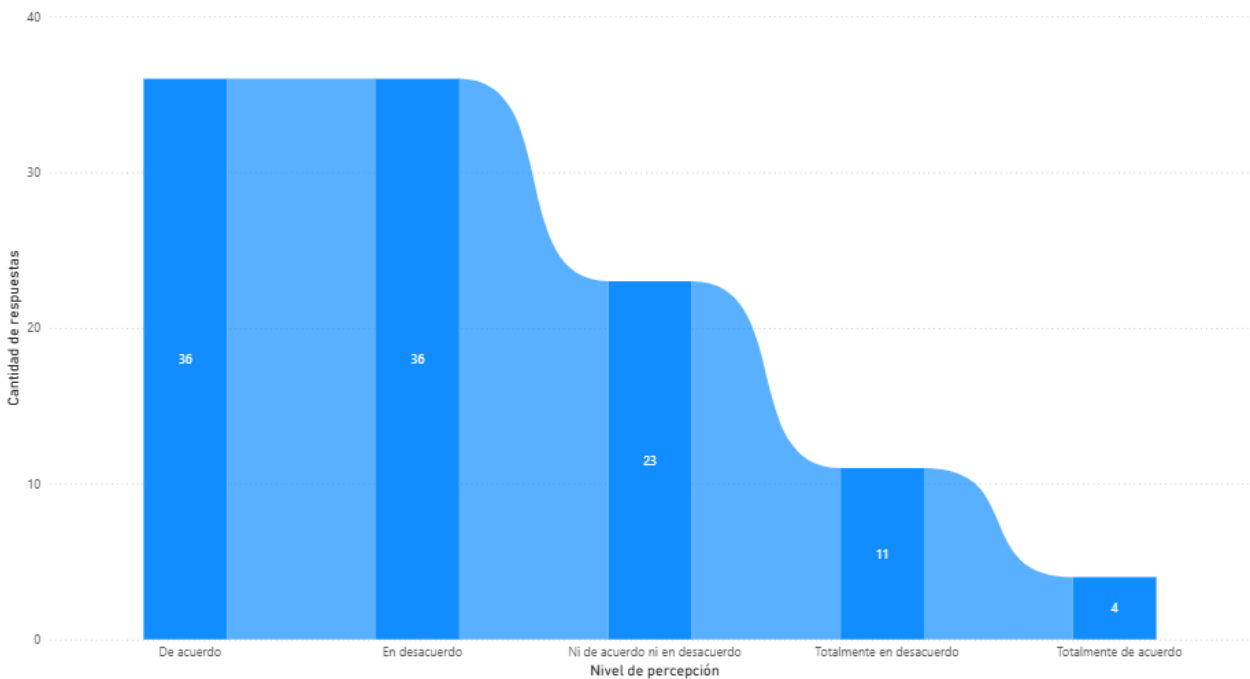
Un total de 61 participantes expresó una valoración favorable a la afirmación: 46 indicaron estar de acuerdo y 15 totalmente de acuerdo, equivalentes al 55.45% de la muestra. Además, 25 colaboradores (22.73%) se mantuvieron neutrales y 24 (21.82%) manifestaron desacuerdo.

La falta de un canal único no debe interpretarse solo como un problema de comodidad para el usuario. En un entorno bancario, la dispersión de canales afecta la trazabilidad, la evidencia del caso, la medición de tiempos y la capacidad de auditoría interna. La Comisión Nacional de Bancos y Seguros (2022). exige a las instituciones supervisadas fortalecer la gestión de tecnologías de información, ciberseguridad y continuidad del negocio; por ello, un canal único contribuye a dejar evidencia, controlar responsabilidades y disminuir la exposición operativa asociada a registros dispersos. Martínez Dubón y Andrade Suazo (2021) encontraron una situación comparable en la Secretaría de Gobernación, Justicia y Descentralización, donde la ausencia de un

“único punto de contacto” impedía conocer con precisión la cantidad de requerimientos recibidos y limitaba la generación de reportes para la toma de decisiones.

La centralización no debe presentarse únicamente como una mejora de comodidad. También es una medida de gobernanza. Utilizar un flujo formal para las incidencias de software en una mesa de ayuda cumple una función crítica dentro de ITSM, ya que su efectividad depende de una coordinación organizacional adecuada. (AXELOS, 2019)

Gráfico 17: El proceso actual descentralizado (usar Teams, correo o WhatsApp) para reportar problemas me resulta confuso o ineficiente.



Fuente: Elaboración Propia.

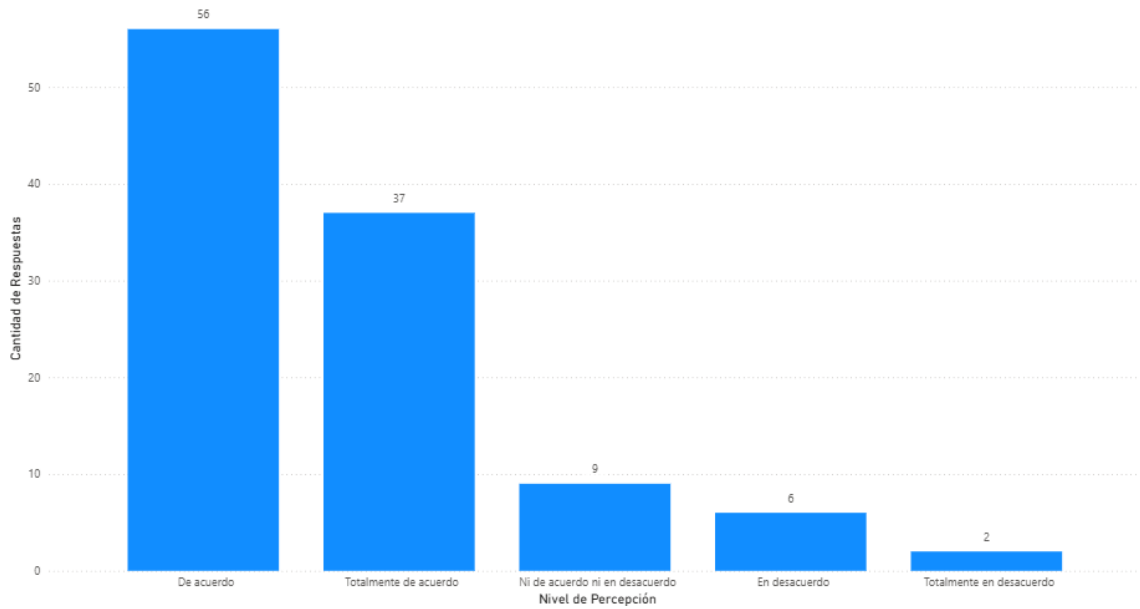
Un total de 40 colaboradores manifestó que el proceso descentralizado le resulta confuso o ineficiente: 36 indicaron estar de acuerdo y 4 totalmente de acuerdo, equivalentes al 36.36% de la muestra. Por otra parte, 23 participantes (20.91%) se mantuvieron neutrales y 47 (42.73%) expresaron desacuerdo.

Las respuestas están divididas. Una parte de los usuarios no considera confuso el esquema actual, posiblemente porque ya conoce a quién contactar y ha desarrollado sus propios atajos. Sin embargo, esa aparente facilidad puede fallar cuando el caso requiere seguimiento, reasignación o evidencia histórica. Un proceso institucional no debería depender del conocimiento personal de cada colaborador. En Banco Ficensa, el reto es conservar la cercanía de atención sin sacrificar

trazabilidad, medición ni control. Rodríguez Archaga (2024), en su estudio sobre Industrias Pacer, también relacionó la falta de una mesa de servicio formal con desorganización en el seguimiento y resolución de problemas, afectando la productividad y la percepción del soporte técnico.

La propuesta no se justifica solo por la percepción de confusión, sino por la necesidad de ordenar el ciclo completo de la incidencia de software. La adopción de un flujo formal para reportar las incidencias de software varía según el contexto. En este caso, conviene conservar la facilidad de contacto y agregar controles que reduzcan la dependencia de prácticas informales. La propuesta debe conservar la facilidad de contacto que valoran los usuarios, pero trasladar el registro, seguimiento y cierre hacia un sistema formal. Esto permite equilibrar cercanía operativa con trazabilidad institucional, elemento relevante para avanzar hacia una mayor madurez ITSM (Marrone y otros, 2014)

Gráfico 18: Un sistema centralizado de atención mejoraría la trazabilidad y control de las incidencias de software.



Fuente: Elaboración Propia.

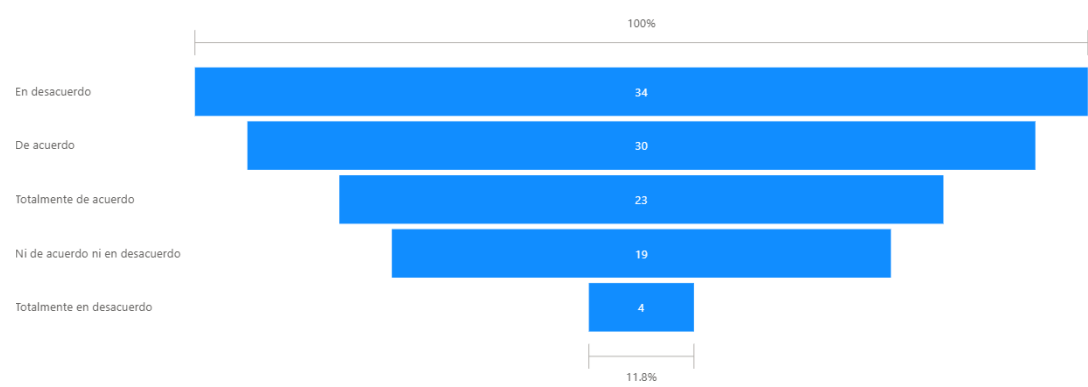
Un total de 93 colaboradores manifestó una valoración favorable: 56 indicaron estar de acuerdo y 37 totalmente de acuerdo, equivalentes al 84.55% de la muestra. Además, 9 participantes (8.18%) se mantuvieron neutrales y 8 (7.27%) expresaron desacuerdo.

Este gráfico conecta directamente con la propuesta de investigación. Desde el punto de vista operativo, un sistema centralizado ordena el registro y seguimiento; desde la perspectiva del

negocio, permite convertir las incidencias en datos útiles para priorizar inversiones, identificar sistemas críticos, medir desempeño y reducir riesgos. La literatura sobre ITSM señala que la adopción de ITIL se asocia con mayor formalización, medición y madurez del servicio (Marrone y otros, 2014) Esta idea se complementa con COBIT 2019, al entender el sistema centralizado como un mecanismo de gobierno y no solo como un repositorio de tickets ISACA (2018). La evidencia de tesis similares respalda este resultado: Martínez Dubón y Andrade Suazo (2021) concluyeron que implementar un Service Desk era factible para mejorar eficiencia, satisfacción y automatización de procesos, mientras que Almendarez Rodríguez y Cuellar Varela (2024) vincularon una mesa de servicio optimizada con estadísticas más claras y mejor percepción del cliente interno.

El hallazgo estratégico es que existe aceptación interna para avanzar hacia una gestión más formal. Esta aceptación reduce el riesgo de resistencia al cambio y permite justificar la implementación gradual de una Mesa de Servicio para incidencias de software. Además, al relacionarse con COBIT 2019, el sistema centralizado puede funcionar como mecanismo de gobierno, medición y control, no solo como repositorio de tickets ISACA (2018).

Gráfico 19: La existencia de varios canales para reportar incidencias (Teams, WhatsApp, Correo, etc.) me genera confusión.



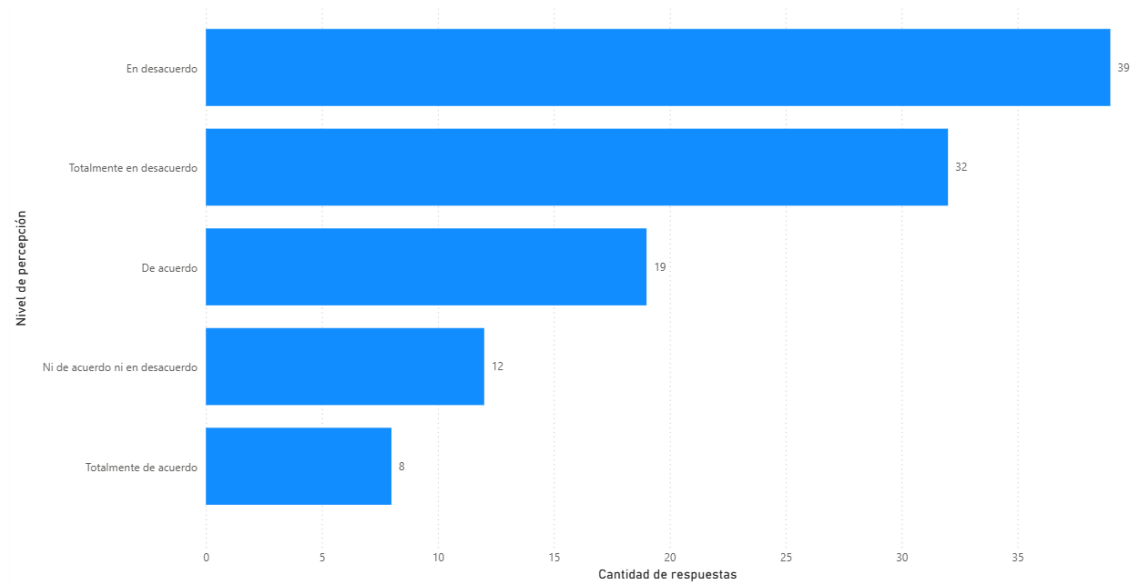
Fuente: Elaboración Propia.

Un total de 53 colaboradores indicó que la existencia de varios canales genera confusión: 30 respondieron estar de acuerdo y 23 totalmente de acuerdo, equivalentes al 48.18% de la muestra. Asimismo, 19 participantes (17.27%) se mantuvieron neutrales y 38 (34.55%) manifestaron desacuerdo.

El dato revela una situación mixta: algunos usuarios se adaptan a los canales actuales, mientras otros experimentan incertidumbre. Desde una mirada estratégica, el problema no es únicamente que existan varios medios, sino que no todos garantizan el mismo nivel de trazabilidad, clasificación, medición y cierre. Por ello, la multiplicidad de canales solo resulta viable si existe un punto formal donde toda incidencia quede registrada y pueda ser auditada posteriormente. Esta situación se relaciona con lo observado por Rodríguez Archaga (2024) en su estudio sobre Industrias Pacer quien identificó como áreas críticas la ausencia de un sistema centralizado y la falta de indicadores clave de rendimiento para controlar la atención de solicitudes.

el banco necesita un criterio común de entrada para todas las incidencias de software. Aunque se mantengan medios alternativos para comunicación rápida, el registro oficial debería centralizarse. De esta forma, los usuarios conservarían agilidad, pero el banco ganaría control, medición y memoria histórica del proceso, elementos claves de una gestión de servicios orientada al negocio (Stuart D. Galup, 2009).

Gráfico 20: He tenido que reportar la misma falla de software más de una vez en un período de 30 días.



Fuente: Elaboración Propia.

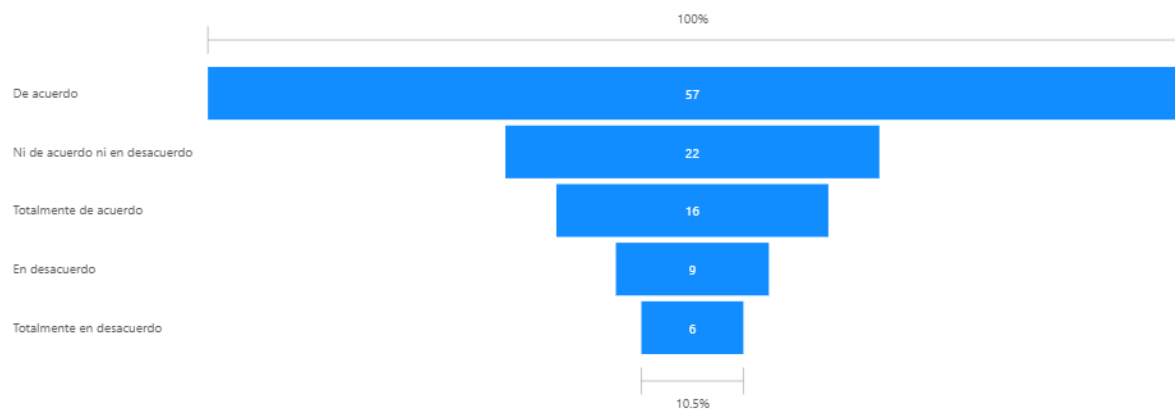
Un total de 27 colaboradores indicó haber reportado la misma falla más de una vez en un período de 30 días: 19 respondieron estar de acuerdo y 8 totalmente de acuerdo, equivalentes al 24.55% de la muestra. Además, 12 participantes (10.91%) se mantuvieron neutrales y 71 (64.55%)

manifestaron desacuerdo.

La reincidencia percibida por los usuarios debe analizarse con cuidado porque puede estar asociada a soluciones temporales, causas raíz no identificadas o cierres realizados sin validación suficiente. (AXELOS, 2019) diferencia la gestión de incidencias, enfocada en restaurar el servicio, de la gestión de problemas, orientada a identificar causas raíz y reducir recurrencias. Por eso, cuando la misma falla se reporta varias veces, el caso deja de ser únicamente operativo y se convierte en una señal de deuda técnica, riesgo de productividad y necesidad de análisis estructural. En trabajos similares sobre Service Desk, la gestión de incidentes no se analiza de forma aislada, sino junto con la gestión de problemas y la generación de información histórica para prevenir repeticiones Martínez Dubón y Andrade Suazo (2021).

El hallazgo es que los casos repetitivos deben recibir un tratamiento distinto al de una incidencia aislada. La propuesta debe incluir una regla para identificar reincidencias, escalar los casos a análisis de problema y documentar acciones correctivas. Esto permitiría reducir costos indirectos asociados a reprocesos, interrupciones repetidas y pérdida de productividad de los usuarios internos. Este tratamiento es coherente con la recomendación de medir indicadores de incidentes, reincidencias y tiempos de atención como base para mejorar el desempeño del servicio (ManageEngine, 2024).

Gráfico 21: Las soluciones brindadas por TI suelen ser definitivas y evitan que tenga que volver a reportar la misma falla poco tiempo después.



Fuente: Elaboración Propia.

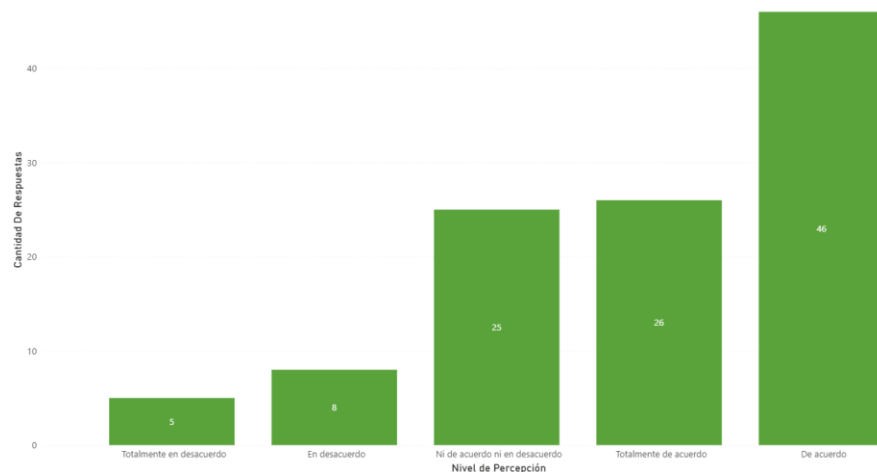
Un total de 73 colaboradores manifestó una percepción favorable: 57 indicaron estar de acuerdo y 16 totalmente de acuerdo, equivalentes al 66.36% de la muestra. Por otro lado, 22

participantes (20.00%) se mantuvieron neutrales y 15 (13.64%) expresaron una valoración desfavorable.

Aunque el dato mayoritario es favorable, el grupo neutral y desfavorable muestra que no todos los usuarios perciben soluciones concluyentes. Esta situación puede relacionarse con cierres prematuros, falta de validación del usuario o atención enfocada en resolver el síntoma sin revisar la causa. Pujay Iglesias y León (2019) muestran que la implementación de modelos basados en ITIL puede contribuir a mejorar la atención de incidentes cuando se estructuran actividades, responsabilidades y criterios de seguimiento. Por tanto, la percepción de solución definitiva debe contrastarse con evidencia de cierre, recurrencia y validación. Castro Martínez y Gómez Hernández (2018) en su estudio en una institución financiera refuerzan esta idea al señalar que atender un ticket dentro del plazo no siempre garantiza que la solución brindada haya sido la adecuada; por ello, la calidad del cierre debe validarse con el usuario.

El hallazgo estratégico es que la calidad de la solución debe medirse, no asumirse. El modelo propuesto debería incorporar validación de cierre, descripción de la solución aplicada, revisión de reincidencias y aprendizaje documentado. Esto ayudaría a diferenciar entre una incidencia atendida y una incidencia realmente resuelta, aspecto clave para mejorar la productividad y la confianza de las áreas usuarias. (Quiñónez Ku, 2018).

Gráfico 22: El personal de TI muestra disposición para atender los problemas reportados.



Fuente: Elaboración Propia.

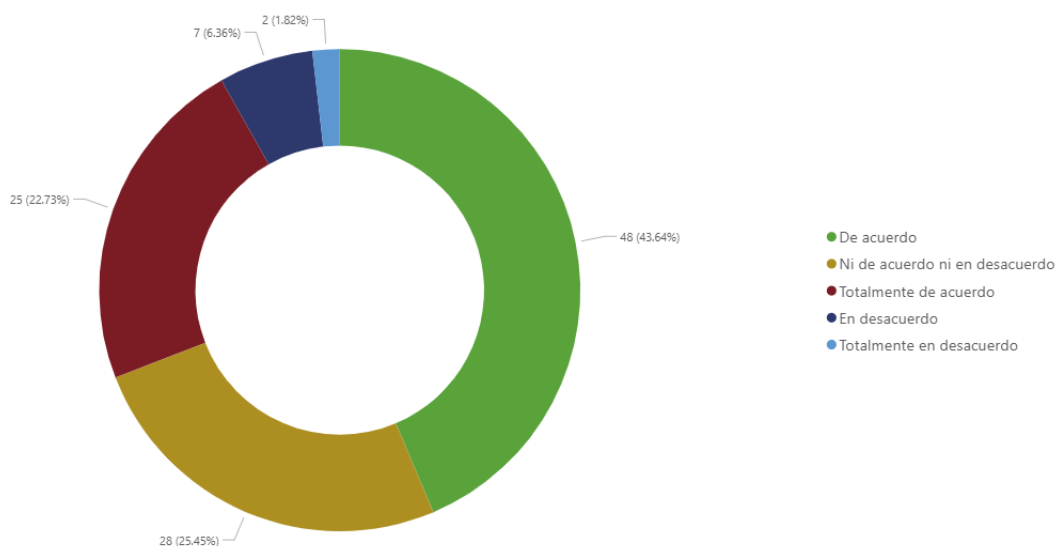
Un total de 72 colaboradores expresó una valoración favorable sobre la disposición del personal de TI: 46 indicaron estar de acuerdo y 26 totalmente de acuerdo, equivalentes al 65.45%

de la muestra. Además, 25 participantes (22.73%) se mantuvieron neutrales y 13 (11.82%) manifestaron una percepción desfavorable.

La disposición del personal de TI es valorada positivamente y representa una fortaleza. Sin embargo, casi una cuarta parte de los usuarios se mantiene neutral, lo que indica que la experiencia no siempre es uniforme. Esto puede depender del canal utilizado, la carga de trabajo o la disponibilidad de la persona contactada. Cuando la atención depende de relaciones individuales, el servicio puede variar según el punto de entrada.

La buena disposición del equipo debe traducirse en una capacidad institucional estable. ITIL 4 resalta la dimensión de organizaciones y personas; por ello, el modelo debe establecer roles, tiempos esperados y reglas de escalamiento.

Gráfico 23: Las soluciones brindadas por TI suelen ser claras y fáciles de comprender.



Fuente: Elaboración Propia.

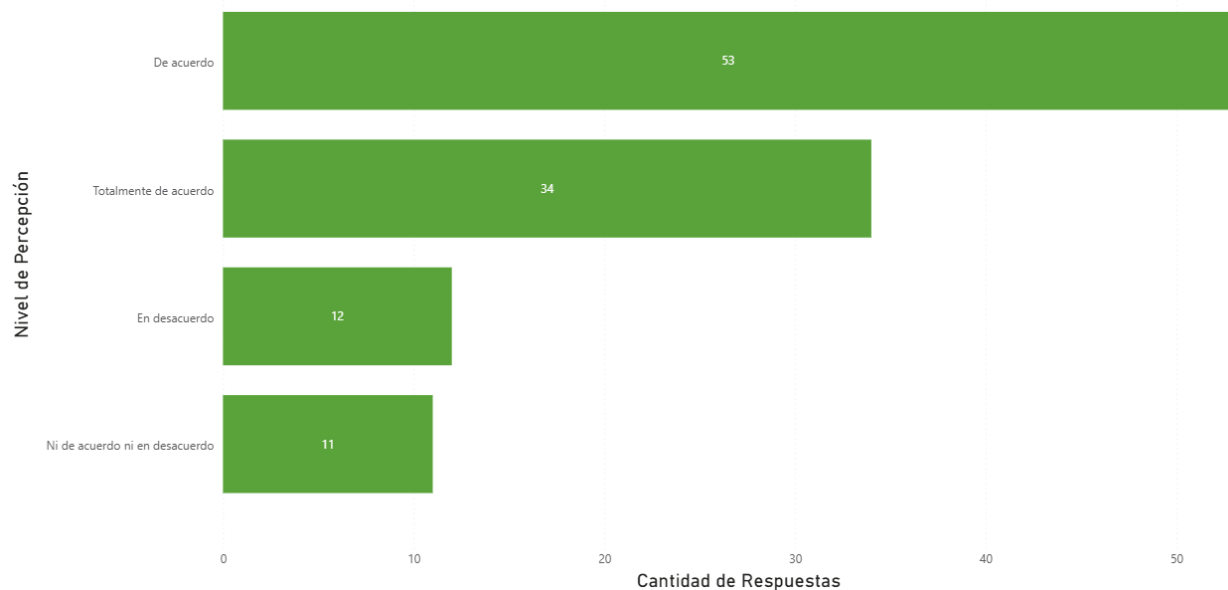
Un total de 73 colaboradores manifestó una valoración favorable: 48 indicaron estar de acuerdo y 25 totalmente de acuerdo, equivalentes al 66.36% de la muestra. Asimismo, 28 participantes (25.45%) se mantuvieron neutrales y 9 (8.18%) expresaron una percepción desfavorable.

Aunque la mayoría comprende las soluciones, una cuarta parte no expresa una opinión claramente favorable. En algunos casos, el cierre puede comunicarse con términos demasiado

técnicos o variar según la persona que atendió la incidencia. Una solución correcta pierde parte de su valor si el usuario no entiende qué ocurrió, qué debe hacer o cómo reconocer si la falla reaparece.

El cierre debe ser claro, breve y útil para el usuario. La propuesta debería incluir plantillas de resolución y una base de conocimiento con respuestas reutilizables. Esto se relaciona con el principio de ITIL 4 de enfocarse en el valor: la solución no solo debe funcionar, también debe ser comprensible.

Gráfico 24: Considero que el personal de TI tiene la capacidad técnica necesaria para resolver las incidencias de software que reporto.



Fuente: Elaboración Propia.

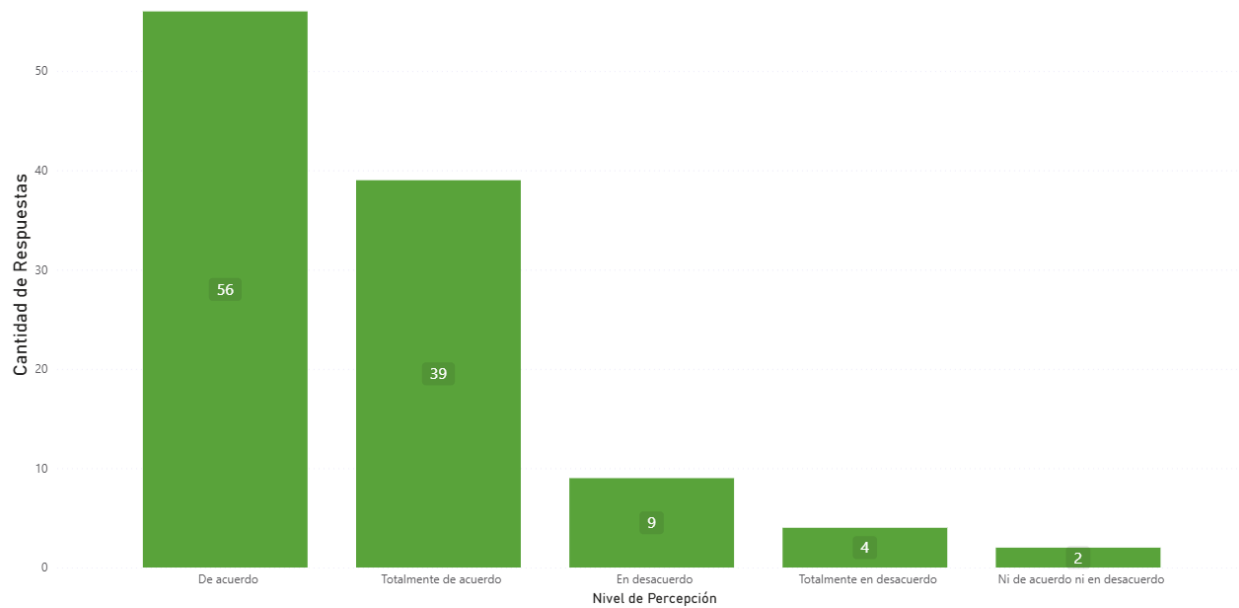
Un total de 87 participantes manifestó una percepción favorable sobre la capacidad técnica del personal de TI: 53 indicaron estar de acuerdo y 34 totalmente de acuerdo, equivalentes al 79.09% de la muestra. Además, 11 colaboradores (10.00%) se mantuvieron neutrales y 12 (10.91%) expresaron desacuerdo. Ningún participante seleccionó la opción totalmente en desacuerdo.

Este resultado permite separar con mayor claridad el problema técnico del problema de gestión. Los usuarios reconocen la capacidad del equipo de TI, pero incluso un personal competente enfrenta dificultades cuando recibe solicitudes dispersas, información incompleta o prioridades definidas de manera desigual. La fortaleza técnica existe; lo que falta es un proceso

que la respalde.

La propuesta debe concentrarse en ordenar el proceso, fortalecer la herramienta y mejorar la gobernanza, sin presentar la situación como una carencia general de conocimiento técnico.

Gráfico 25: Cuando reporto una incidencia, generalmente logro indicar con claridad el nivel de urgencia o impacto que tiene en mis funciones.



Fuente: Elaboración Propia.

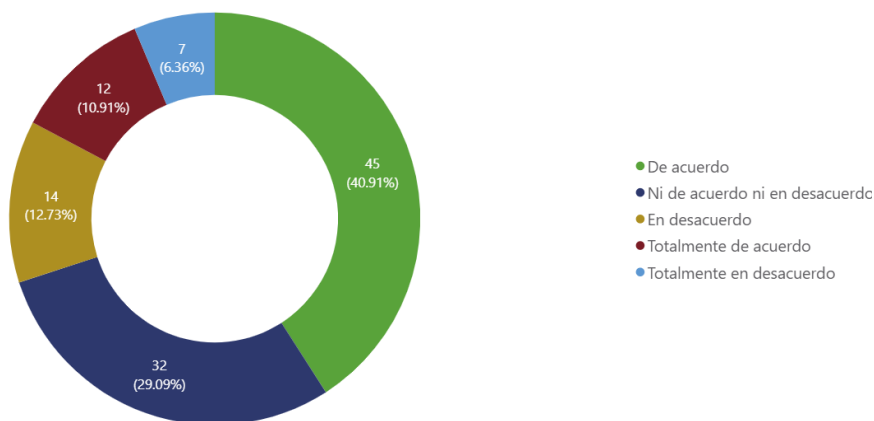
Un total de 95 colaboradores manifestó una percepción favorable: 56 indicaron estar de acuerdo y 39 totalmente de acuerdo, equivalentes al 86.36% de la muestra. Además, 2 participantes (1.82%) se mantuvieron neutrales y 13 (11.82%) expresaron desacuerdo.

Este es uno de los resultados que más requiere fortalecimiento analítico. La mitad de la muestra no confirma plenamente que la priorización responda a la criticidad del negocio. En banca, esta situación es delicada porque una incidencia de software puede afectar operaciones, reportes regulatorios, atención al cliente o procesos de cierre. De acuerdo con ISACA (2018) , el gobierno de TI debe asegurar beneficios, optimizar riesgos y entregar servicios conforme a los requerimientos del negocio. Por eso, la priorización debe traducir la criticidad tecnológica en criticidad operativa y financiera. La experiencia documentada en Banco Davivienda muestra que la ausencia de priorización y clasificación estructurada afecta la gestión de incidentes y solicitudes, por lo que la criticidad debe traducirse en reglas claras de atención y escalamiento Almendarez

Rodríguez y Cuellar Varela (2024)

La matriz debe considerar impacto operativo, urgencia, número de usuarios afectados, proceso bancario involucrado, riesgo regulatorio y continuidad del servicio. Esto permitiría que las incidencias no se atiendan solo por orden de llegada, sino por su impacto real sobre la operación institucional (Comisión Nacional de Bancos y Seguros, 2022; ISO, 2018).

Gráfico 26: Considero que el área de TI prioriza adecuadamente las incidencias según su nivel de criticidad para el negocio.



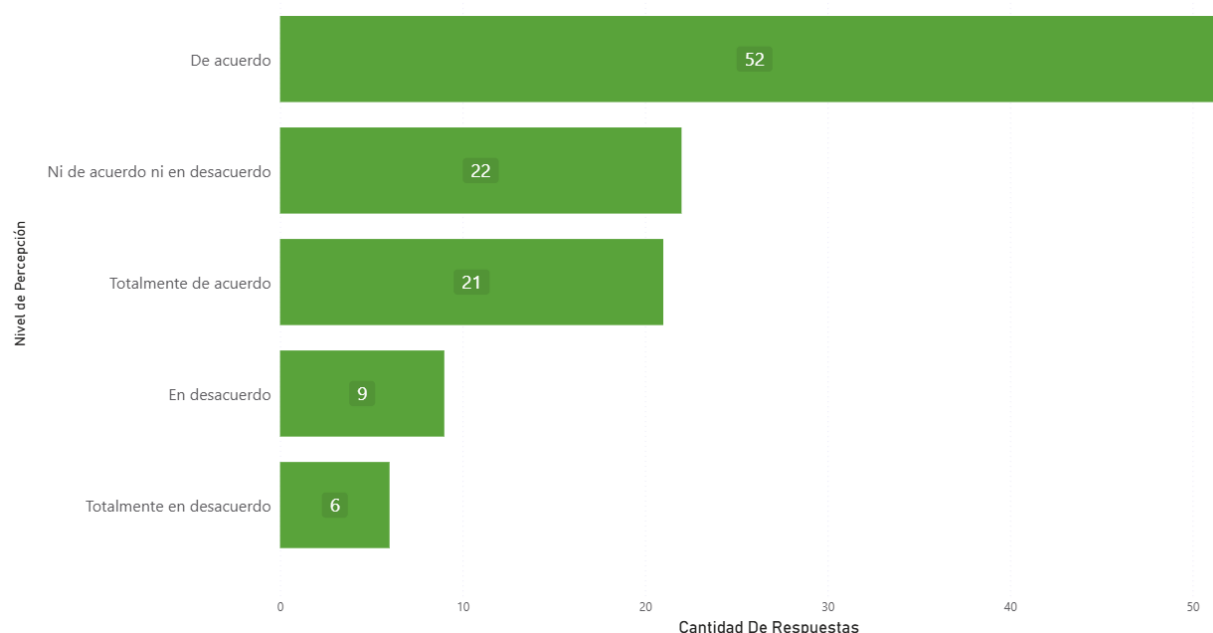
Fuente: Elaboración Propia.

Un total de 57 colaboradores manifestó una percepción favorable: 45 indicaron estar de acuerdo y 12 totalmente de acuerdo, equivalentes al 51.82% de la muestra. Por otra parte, 32 participantes (29.09%) se mantuvieron neutrales y 21 (19.09%) expresaron una valoración desfavorable.

Este es uno de los resultados con menor aprobación en toda la encuesta. Casi la mitad de los usuarios no confirma que la priorización sea adecuada. La causa puede estar en la falta de criterios visibles o en reportes que llegan sin suficiente información sobre el impacto. Si la prioridad no se define con una regla común, el banco se expone a retrasar casos críticos y a utilizar sus recursos de manera poco eficiente.

La matriz de prioridad debe ocupar un lugar central en el modelo. ITIL 4 propone valorar impacto y urgencia, mientras que COBIT 2019 refuerza la necesidad de procesos e información confiable para tomar decisiones consistentes. Estos criterios deben ser conocidos tanto por los usuarios como por los responsables de TI.

Gráfico 27: Cuando reporto una falla, suelo indicar si afecta a otras personas o áreas además de la mía.



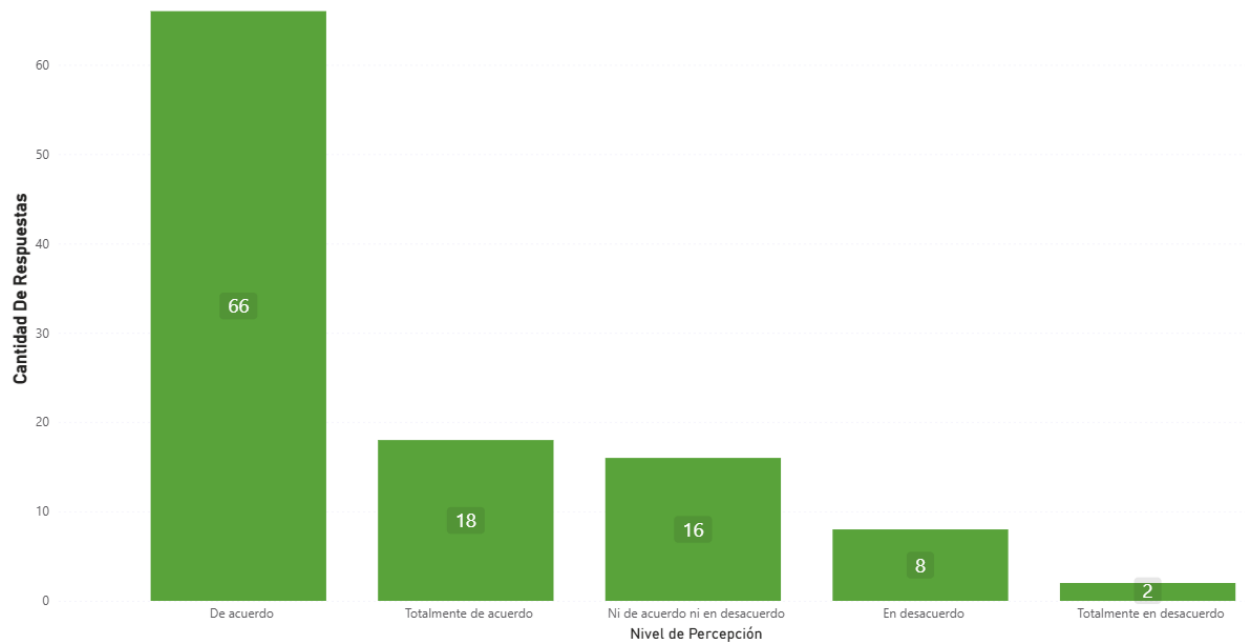
Fuente: Elaboración Propia.

Un total de 73 colaboradores manifestó una percepción favorable: 52 indicaron estar de acuerdo y 21 totalmente de acuerdo, equivalentes al 66.36% de la muestra. Asimismo, 22 participantes (20.00%) se mantuvieron neutrales y 15 (13.64%) expresaron desacuerdo.

La mayoría afirma que comunica si la falla afecta a otras personas o áreas, pero todavía existe una proporción relevante que no lo confirma. Esto puede ocurrir porque los canales actuales no incluyen preguntas específicas o porque el usuario no conoce el alcance completo del problema. Sin esa información, el equipo técnico puede asignar una prioridad menor a la necesaria.

El formulario debería guiar al usuario con preguntas concretas: áreas afectadas, cantidad estimada de personas, proceso comprometido y existencia de una alternativa temporal. Una captura más uniforme mejoraría la clasificación inicial y reduciría la necesidad de solicitar información adicional.

Gráfico 28: En términos generales, me encuentro satisfecho con la forma en que se gestionan actualmente las incidencias de software en Banco Ficensa.



Fuente: Elaboración Propia.

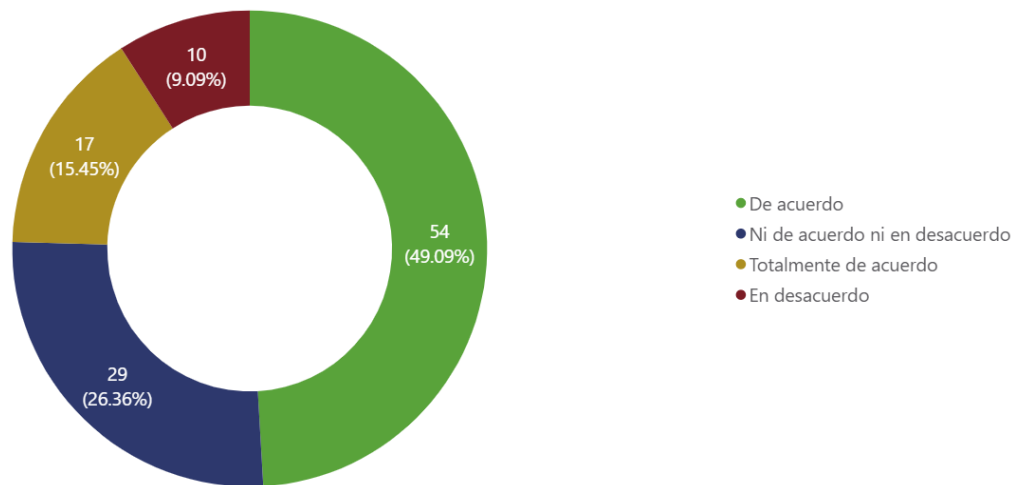
Un total de 84 colaboradores manifestó una valoración favorable sobre su satisfacción general: 66 indicaron estar de acuerdo y 18 totalmente de acuerdo, equivalentes al 76.36% de la muestra. Además, 16 participantes (14.55%) se mantuvieron neutrales y 10 (9.09%) expresaron una valoración desfavorable.

La satisfacción general es favorable, pero no significa que el proceso ya esté resuelto. Los gráficos anteriores muestran dificultades puntuales en seguimiento, registro, centralización y priorización. Es probable que los usuarios valoren la disposición del equipo técnico aun cuando la atención continúe apoyándose en prácticas informales. La percepción positiva y las brechas de control pueden coexistir.

La propuesta debería conservar las fortalezas actuales y reducir la variabilidad del proceso. Es importante estandarizar como se atienden las incidencias de software en el contexto bancario.

Gráfico 29: El servicio que recibo por parte de TI cuando reporto incidencias de software

cumple con mis expectativas.



Fuente: Elaboración Propia.

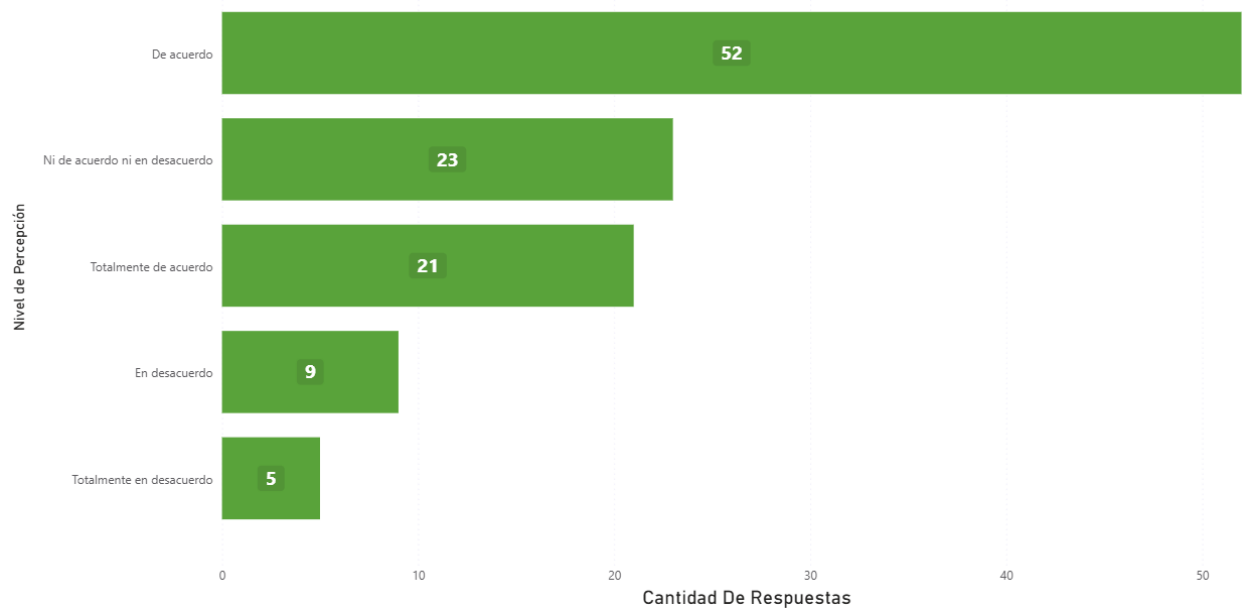
Un total de 71 colaboradores manifestó una percepción favorable: 54 indicaron estar de acuerdo y 17 totalmente de acuerdo, equivalentes al 64.55% de la muestra. Por otro lado, 29 participantes (26.36%) se mantuvieron neutrales y 10 (9.09%) expresaron desacuerdo. Ningún participante seleccionó la opción totalmente en desacuerdo.

La satisfacción general debe interpretarse como una señal de que el área de TI cuenta con reconocimiento interno, pero no necesariamente como evidencia de madurez del proceso. En ocasiones, los usuarios valoran la disposición del personal, aunque el proceso carezca de trazabilidad o indicadores robustos. Tang y Todo (2013) señalan que la organización del Service Desk en iniciativas de ITSM requiere definir estructura, responsabilidades y mecanismos de atención. Por ello, la satisfacción actual debe aprovecharse como base para formalizar el proceso, no como razón para mantenerlo sin cambios. Este resultado guarda relación con el estudio realizado en BAC Credomatic, donde la percepción del usuario interno fue tratada como un elemento clave para comprender la efectividad real del área de TI, más allá del cumplimiento operativo de tickets (Castro Martínez & Gómez Hernández, 2018).

La propuesta debe conservar las fortalezas actuales del servicio, especialmente la disposición y capacidad de respuesta del equipo, pero debe reducir la variabilidad mediante reglas formales. El objetivo no es deshumanizar la atención, sino respaldar la buena disposición del personal con un proceso medible, repetible y alineado con las expectativas del banco (Petersen,

2019).

Gráfico 30: Me siento confiado al reportar incidencias de software al área de TI porque considero que recibiré atención y seguimiento adecuados.



Fuente: Elaboración Propia.

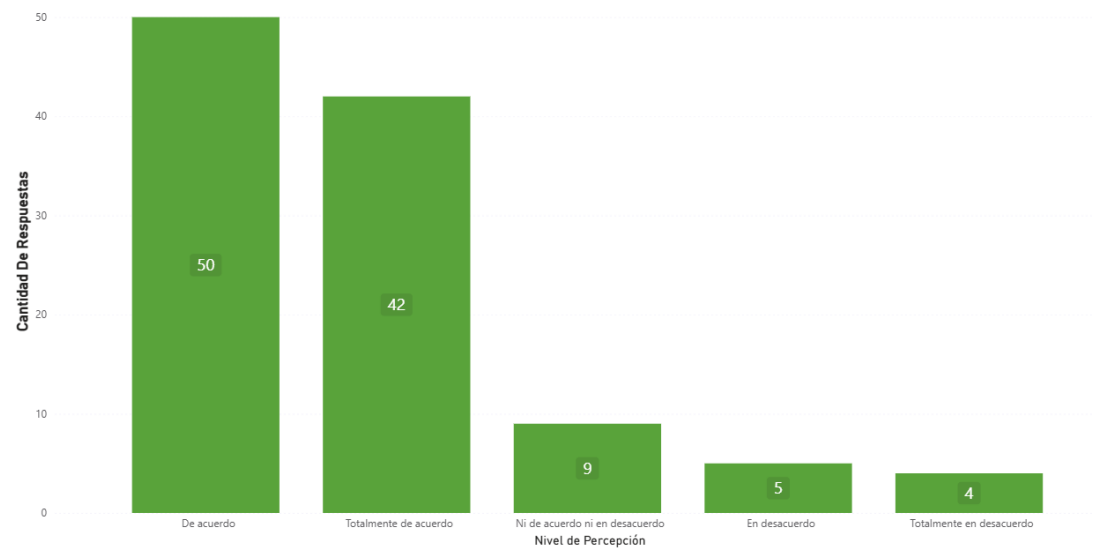
Un total de 73 colaboradores manifestó una percepción favorable: 52 indicaron estar de acuerdo y 21 totalmente de acuerdo, equivalentes al 66.36% de la muestra. Además, 23 participantes (20.91%) se mantuvieron neutrales y 14 (12.73%) expresaron una valoración desfavorable.

Este resultado sugiere que el servicio actual cumple parcialmente con lo esperado, pero todavía existe espacio para alinear mejor las expectativas entre usuarios y TI. Banco Ficensa (2020) definió como objetivo “Mantener altos estándares de niveles de servicio dentro de la Gerencia de Tecnologías de Información y Comunicaciones” (pág. 9). Esto permite vincular el resultado con una expectativa institucional concreta: no basta con atender casos, sino que el servicio debe ser medible, consistente y alineado con estándares internos. En esa misma línea, Almendarez Rodríguez y Cuellar Varela (2024) orientaron la optimización de la Mesa de Servicio de Banco Davivienda a mejorar la eficiencia operativa, la calidad del servicio y la satisfacción del cliente interno.

La propuesta debe definir tiempos esperados por criticidad, comunicación mínima, responsables, escalamiento y criterios de cierre. Esto reduciría ambigüedad y permitiría evaluar el

servicio con base en datos, no solo en percepciones (KnowledgeHut., 2023).

Gráfico 31: Considero que una Mesa de Servicio centralizada mejoraría la gestión de incidencias de software.



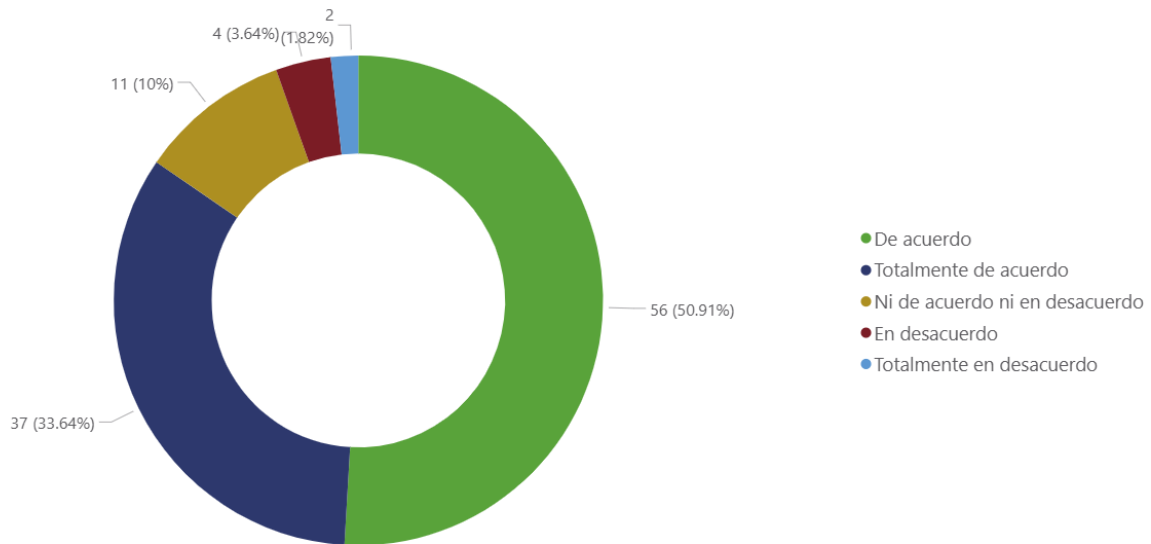
Fuente: Elaboración Propia.

Un total de 92 colaboradores manifestó una percepción favorable: 50 indicaron estar de acuerdo y 42 totalmente de acuerdo, equivalentes al 83.64% de la muestra. Además, 9 participantes (8.18%) se mantuvieron neutrales y 9 (8.18%) expresaron una valoración desfavorable.

El respaldo mayoritario indica que los usuarios ven una oportunidad clara de mejora. Una Mesa de Servicio permitiría centralizar el registro, aplicar categorías comunes y generar información para evaluar el desempeño. Sin embargo, la herramienta por sí sola no resolverá el problema. También deben definirse responsables, prioridades, tiempos y reglas de seguimiento.

La aceptación existente facilita avanzar hacia una un flujo formal en la Mesa de Servicio recuerda que su funcionamiento depende de la coordinación organizacional. La implementación debe integrar personas, procesos y tecnología.

Gráfico 32: Utilizaría con frecuencia una Mesa de Servicio centralizada si estuviera disponible para reportar incidencias de software.



Fuente: Elaboración Propia.

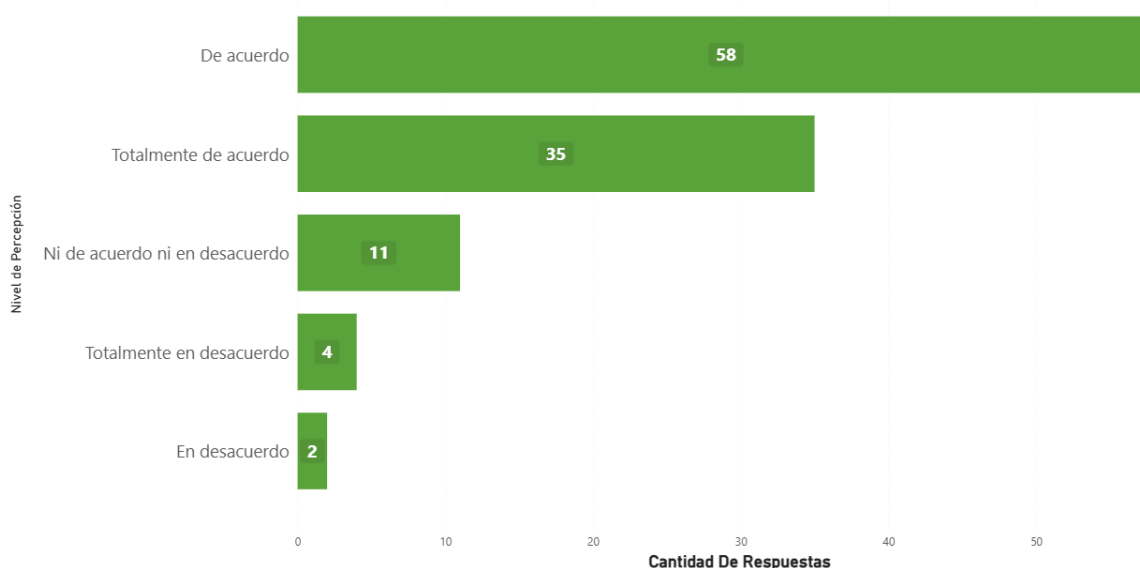
Un total de 93 colaboradores manifestó intención favorable de uso: 56 indicaron estar de acuerdo y 37 totalmente de acuerdo, equivalentes al 84.55% de la muestra. Por otra parte, 11 participantes (10.00%) se mantuvieron neutrales y 6 (5.45%) expresaron una valoración desfavorable.

Este resultado constituye un respaldo directo para la propuesta. La Mesa de Servicio no debe entenderse únicamente como una herramienta para registrar tickets, sino como una función estratégica que integra demanda, priorización, comunicación, escalamiento y medición. Petersen (2019) plantea que el desarrollo de un Service Desk requiere coordinación entre personas, procesos y herramientas. En la misma línea, los estudios de implementación de ITIL muestran que la formalización del punto de contacto mejora el seguimiento y contribuye a elevar la calidad del servicio (Ayala Soto & Caso Rojas, 2023). Rodríguez Archaga (2024) coincide al plantear que una mesa de servicio basada en ITIL 4 puede mejorar la eficiencia operativa, la calidad del servicio y la satisfacción de los usuarios internos cuando se acompaña de capacitación, centralización y medición.

La principal barrera inicial no parece ser la voluntad de los usuarios, sino la capacidad

institucional para sostener el nuevo procedimiento. La adopción de ITIL requiere gestión del cambio. Por ello, la puesta en marcha debería incluir comunicación, capacitación y seguimiento del uso. La organización tiene condiciones favorables para incorporar las incidencias de software a una Mesa de Servicio centralizada. Para que el beneficio sea real, la implementación debe incluir catálogo de servicios, criterios de criticidad, responsables, SLA, tablero de indicadores y reglas de cierre. De esta forma, la Mesa de Servicio se convierte en una fuente de gobierno y aprendizaje organizacional. (ISACA, 2018)

Gráfico 33: Considero que contar con un canal único y formal para reportar incidencias mejoraría mi experiencia de atención.



Fuente: Elaboración Propia.

Un total de 93 colaboradores manifestó una percepción favorable: 58 indicaron estar de acuerdo y 35 totalmente de acuerdo, equivalentes al 84.55% de la muestra. Asimismo, 11 participantes (10.00%) se mantuvieron neutrales y 6 (5.45%) expresaron una valoración desfavorable.

La alta intención de uso reduce el riesgo de rechazo inicial y permite anticipar una adopción favorable. Sin embargo, la adopción no debe darse por garantizada. Si el sistema resulta complejo, lento o no ofrece seguimiento visible, los usuarios podrían regresar a canales informales. AXELOS (2019) resalta la importancia de la co-creación de valor en la gestión de servicios; aplicado a este caso, la Mesa de Servicio debe diseñarse con participación de usuarios de Negocios

y Operaciones para asegurar que sea útil, clara y fácil de adoptar. La adopción esperada debe acompañarse de gestión del cambio, porque estudios previos han identificado que la capacitación de usuarios y técnicos es necesaria para sostener una mesa de servicio funcional y evitar el retorno a prácticas informales (Martínez Dubón & Andrade Suazo , 2021).

La propuesta cuenta con aceptación potencial, pero requiere gestión del cambio. Se recomienda acompañar la implementación con comunicación interna, instructivos simples, capacitación a usuarios clave y monitoreo de adopción. Esto ayudaría a convertir la intención de uso en práctica real y sostenida, alineada con la mejora continua propuesta por ITIL 4 (AXELOS, 2019).

4.2.2. ANÁLISIS DE LA MATRIZ DOCUMENTAL DE INCIDENCIAS DE SOFTWARE DEL AÑO 2025

La Matriz Documental de Incidencias de Software constituye el instrumento central de recolección de datos primarios de naturaleza cuantitativa y documental empleado en la presente investigación. Su construcción respondió a la necesidad de sistematizar, en un único instrumento de análisis, el conjunto de registros de incidencias de software gestionadas en Banco Ficensa durante el período comprendido entre enero y diciembre de 2025.

Como instrumento unitario, la matriz recoge variables que permiten caracterizar de manera integral el comportamiento del proceso de gestión de incidencias, entre ellas: fecha de reporte, área funcional afectada, sistema involucrado, tipo de incidencia, medio de reporte utilizado, nivel de criticidad asignado, estado de resolución, condición de reincidencia, tipo de registro empleado, tiempo de atención y tiempo de resolución correspondiente a cada caso.

La articulación de estas variables dentro de un único instrumento responde directamente a los objetivos específicos relacionados con el análisis de la situación actual del proceso, el cálculo de los tiempos de atención y resolución, la clasificación y cuantificación de las incidencias por tipo, criticidad y área afectada, así como la determinación del porcentaje de incidencias gestionadas sin registro formal. Asimismo, los resultados obtenidos sirven como base para el establecimiento de indicadores clave de desempeño y para la formulación posterior de un flujo formal de gestión de incidencias de software alineado con ITIL 4 y complementado con principios de gobierno de TI de COBIT 2019.

En total, el instrumento recoge 56 incidencias de software registradas durante el año 2025 en las dos áreas funcionales objeto de estudio: Negocios y Operaciones. Este universo constituye la base documental a partir de la cual se derivan los análisis subsiguientes. La delimitación del análisis a estas dos áreas es coherente con el alcance definido en la investigación, el cual circunscribe el estudio a las incidencias de software que afectan directamente a las áreas de Negocios y Operaciones del Banco Ficensa. [\(Ver Anexo 6\).](#)

4.2.2.1.VOLUMEN TOTAL Y DISTRIBUCIÓN TEMPORAL DE INCIDENCIAS

Durante el año 2025 se identificaron y registraron en la Matriz Documental un total de 56 incidencias de software correspondientes a las áreas de Negocios y Operaciones de Banco Ficensa. La distribución mensual de los casos evidencia una presencia sostenida de incidencias a lo largo de todo el año, sin que exista un período de inactividad o ausencia total de reportes. Este comportamiento permite afirmar que las incidencias de software no constituyen eventos aislados, sino una condición operativa recurrente que requiere un mecanismo formal, continuo y medible para su gestión.

En términos de distribución mensual, la matriz documental registra el siguiente comportamiento:

Tabla 21: Distribución de Incidencias por mes Año 2025.

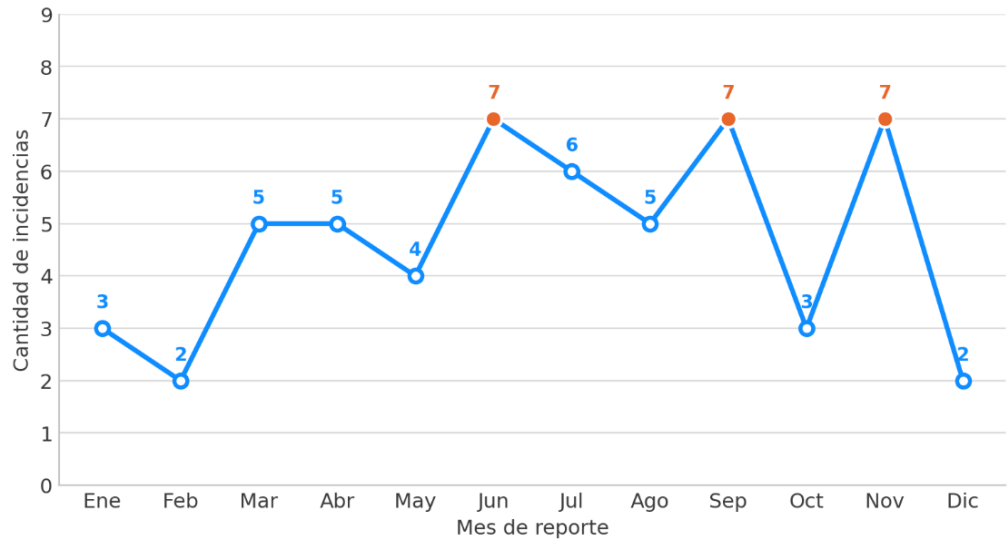
Distribución de Incidencias	
Año 2025	
Mes	Cantidad de Incidencias
Enero	3
Febrero	2
Marzo	5
Abril	5
Mayo	4
Junio	7
Julio	6
Agosto	5
Septiembre	7
Octubre	3
Noviembre	7
Diciembre	2

Fuente: Elaboración Propia

Los meses de junio, septiembre y noviembre registraron el mayor volumen de incidencias, con 7 casos cada uno, mientras que los meses con menor actividad fueron febrero y diciembre, con

2 casos cada uno.

Gráfico 34. Distribución mensual de incidencias de software, año 2025



Fuente: Elaboración propia con base en la Matriz Documental de Incidencias

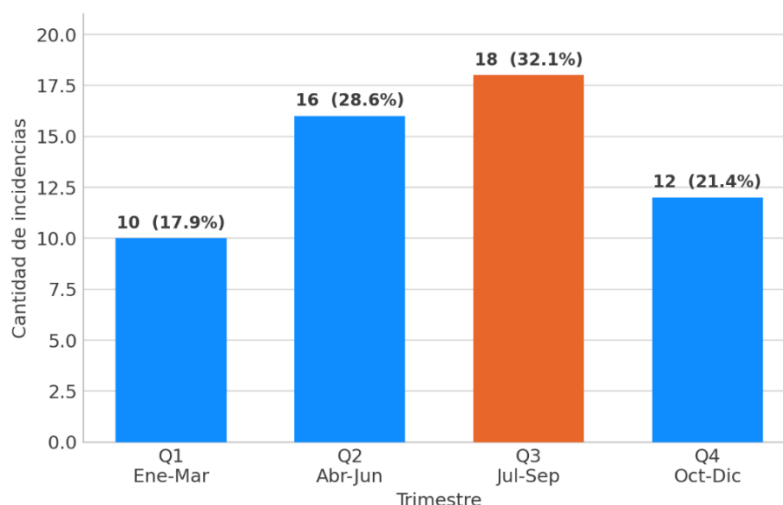
El tercer trimestre del año 2025, correspondiente a los meses de julio, agosto y septiembre, concentró la mayor cantidad de incidencias de software, con 18 casos, equivalentes al 32.1% del total anual. En segundo lugar, se ubicó el segundo trimestre, integrado por abril, mayo y junio, con 16 incidencias, equivalentes al 28.6%. El cuarto trimestre registró 12 casos, correspondientes al 21.4%, mientras que el primer trimestre presentó la menor cantidad de incidencias, con 10 casos, equivalentes al 17.9%.

La distribución trimestral evidencia que las incidencias no se concentraron exclusivamente en un momento aislado del año, debido a que se identificaron casos durante los cuatro trimestres analizados. El análisis documental no permite establecer una causa única para este comportamiento; no obstante, la concentración podría estar asociada con ciclos de procesamiento, cierres internos, actividades regulatorias, integraciones con entidades externas o períodos de mayor demanda operativa.

La gestión de incidencias de software requiere un monitoreo periódico que permita analizar tendencias temporales y anticipar períodos de mayor carga operativa. El modelo propuesto debe facilitar la generación de reportes mensuales y trimestrales, de manera que el área de

Desarrollo pueda identificar variaciones relevantes, priorizar recursos y establecer acciones preventivas cuando se detecten incrementos sostenidos en la cantidad de incidencias.

Gráfico 35. Distribución trimestral de incidencias de software, año 2025



Fuente: Elaboración propia con base en la Matriz Documental de Incidencias

El tercer trimestre del año 2025, correspondiente a los meses de julio, agosto y septiembre, concentró la mayor cantidad de incidencias de software, con 18 casos, equivalentes al 32.1% del total anual. Le siguió el segundo trimestre, integrado por abril, mayo y junio, con 16 incidencias, correspondientes al 28.6%. El cuarto trimestre registró 12 casos, equivalentes al 21.4%, mientras que el primer trimestre presentó la menor cantidad de incidencias, con 10 casos, equivalentes al 17.9%.

La distribución trimestral evidencia que las incidencias de software estuvieron presentes durante todo el año, aunque con una mayor concentración en el segundo y tercer trimestre. Este comportamiento sugiere que la carga operativa no se mantuvo completamente uniforme y que pudieron existir períodos con mayor presión sobre los sistemas utilizados por las áreas de Negocios y Operaciones.

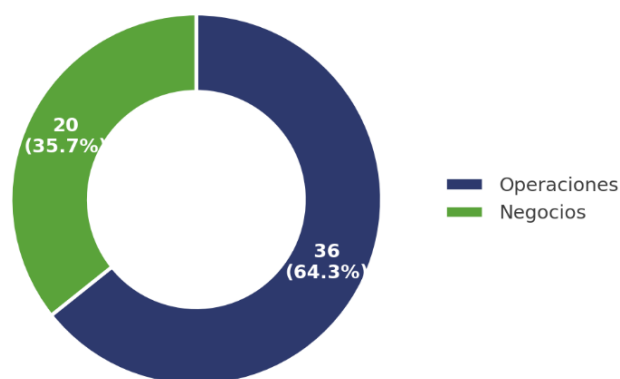
El resultado contribuye al cumplimiento del Objetivo 1, al describir la situación actual de la gestión de incidencias en términos de frecuencia y comportamiento temporal, y aporta al Objetivo 3, al cuantificar su distribución dentro del período analizado. Asimismo, evidencia la necesidad de incorporar mecanismos de seguimiento mensual y trimestral dentro del modelo propuesto. En alineación con ITIL 4, el registro estructurado de las incidencias permitirá

monitorear tendencias, identificar períodos de mayor exposición operativa, establecer prioridades y fortalecer la planificación de la capacidad de respuesta durante todo el año.

4.2.2.2.DISTRIBUCIÓN POR ÁREA FUNCIONAL

El análisis de las tasas de resolución por área funcional evidencia diferencias relevantes. El área de Operaciones resolvió 27 de las 36 incidencias identificadas, alcanzando una tasa de resolución del 75.0%. En contraste, el área de Negocios registró únicamente 1 caso resuelto de un total de 20 incidencias, equivalente a una tasa de resolución del 5.0%. En consecuencia, 19 de las 20 incidencias asociadas con Negocios permanecieron sin una resolución documentada al cierre del período analizado.

Gráfico 36. Distribución de incidencias por área funcional, año 2025.



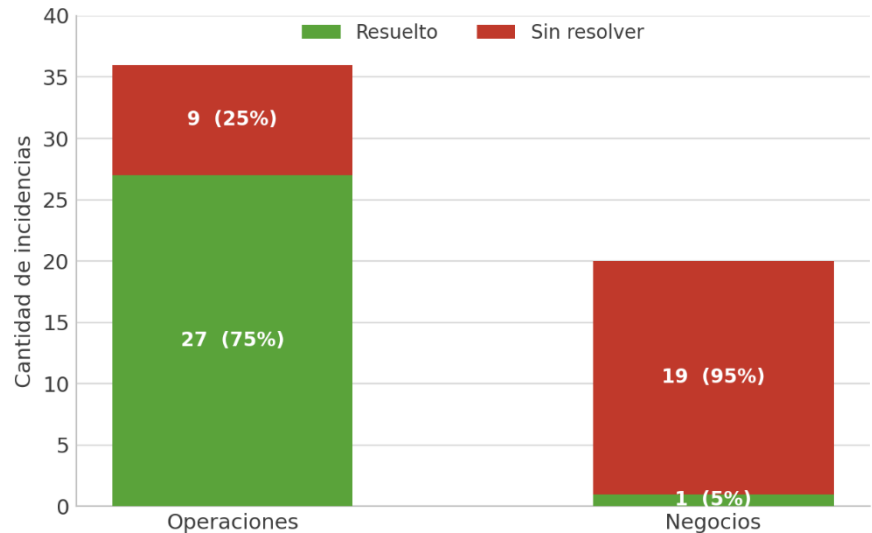
Fuente: Elaboración propia con base en la Matriz Documental de Incidencias

La diferencia entre ambas áreas no debe interpretarse necesariamente como una menor capacidad técnica para atender los casos de Negocios, debido a que la matriz documental no permite determinar por sí sola las causas específicas de esta brecha. No obstante, el comportamiento observado podría estar asociado con una mayor complejidad de las incidencias, dependencias con terceros, ausencia de reglas formales de escalamiento o falta de documentación del cierre. Desde una perspectiva operativa, mantener incidencias abiertas o sin evidencia de solución limita la trazabilidad, dificulta determinar si el servicio fue restaurado y aumenta el riesgo de que las áreas usuarias continúen aplicando soluciones temporales o reportando nuevamente una misma falla.

El hallazgo evidencia que el modelo propuesto debe incorporar mecanismos formales de

seguimiento, actualización de estado, escalamiento y cierre documentado. Además de registrar el inicio de la atención, será necesario identificar los casos que permanecen abiertos durante períodos prolongados y establecer alertas que permitan supervisar su evolución. Esta medida contribuirá a reducir la acumulación de incidencias sin resolución verificable y a fortalecer el control operativo del proceso.

Gráfico 37. Tasa de resolución de incidencias por área funcional, año 2025.



Fuente: Elaboración propia con base en la Matriz Documental de Incidencias.

Esta distribución contribuye al cumplimiento del **Objetivo 1**, al describir la situación actual de la gestión de incidencias en términos de frecuencia, trazabilidad y control operativo por área funcional. Asimismo, aporta al **Objetivo 3**, al clasificar y cuantificar las incidencias según el área afectada. Desde la perspectiva de ITIL 4, identificar las áreas con mayor volumen de incidencias y con mayores brechas de cierre constituye un insumo fundamental para diseñar flujos de atención diferenciados, definir prioridades, asignar responsables y establecer mecanismos de seguimiento más efectivos. En consecuencia, los resultados muestran que el modelo propuesto debe contemplar no solo el volumen de incidencias, sino también la capacidad real de seguimiento y cierre en cada área funcional.

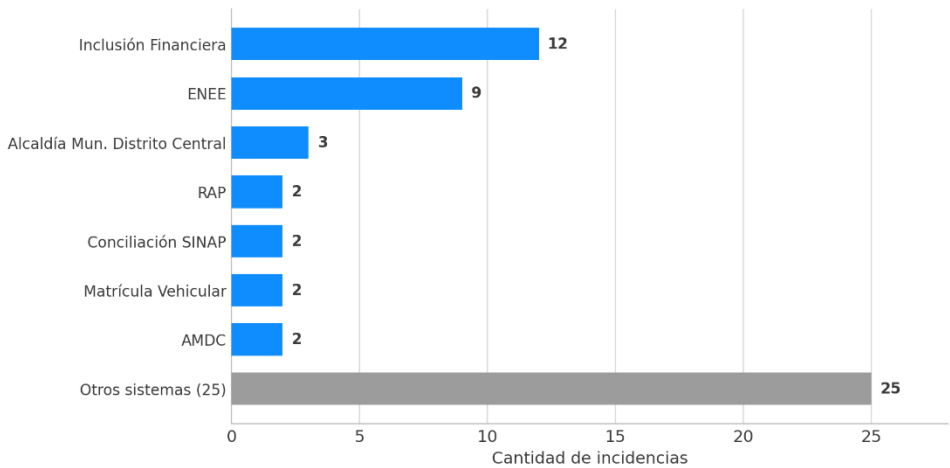
4.2.2.3.DISTRIBUCIÓN POR SISTEMA AFECTADO

Los resultados obtenidos indican que las 56 incidencias registradas involucran una diversidad importante de sistemas, lo cual evidencia una dispersión considerable de la demanda de soporte a través del portafolio de aplicaciones utilizado por Banco Ficensa. No obstante, aunque

las incidencias se distribuyen en múltiples sistemas, también se identifican focos de concentración relevantes que requieren atención prioritaria.

El sistema Inclusión Financiera concentra el mayor número de incidencias, con 12 casos, equivalentes al 21.4% del total. En segundo lugar, se ubica el sistema ENEE, con 9 incidencias, que representan el 16.1%. En un tercer nivel se encuentra Alcaldía Municipal del Distrito Central, con 3 casos, equivalentes al 5.4%. Asimismo, los sistemas RAP, Conciliación SINAP, Matrícula Vehicular y AMDC registran 2 incidencias cada uno, equivalentes al 3.6% por sistema. Los demás sistemas de menor frecuencia acumulan 24 incidencias, equivalentes al 42.9% del total documentado.

Gráfico 38. Sistemas con mayor número de incidencias registradas, año 2025.



Fuente: Elaboración propia con base en la Matriz Documental de Incidencias.

El comportamiento del sistema Inclusión Financiera resulta especialmente relevante dentro del análisis, ya que registra una incidencia por cada mes del año 2025. Los registros asociados a este sistema presentan una descripción recurrente relacionada con errores en la generación de reportes para la Comisión Nacional de Bancos y Seguros (CNBS), derivados de fallas en el software y en la base de datos. Además, la totalidad de estas 12 incidencias se encuentra en estado sin resolver, con atención registrada el mismo día del reporte, pero sin fecha de resolución definitiva documentada.

Este patrón permite identificar una condición de recurrencia que no debe analizarse únicamente como incidentes aislados, sino como una posible problemática repetitiva que requiere revisión técnica y análisis de causa raíz. Desde la perspectiva de ITIL 4, este comportamiento se

relaciona con la necesidad de articular la gestión de incidentes con la gestión de problemas, ya que la atención individual de casos recurrentes puede restaurar temporalmente la operación, pero no necesariamente eliminar la causa que origina la repetición del evento.

De manera similar, el sistema ENEE acumula 9 incidencias durante el período analizado. A diferencia de Inclusión Financiera, los casos asociados a ENEE aparecen como resueltos; sin embargo, una proporción importante de ellos presenta condición de reincidencia. Esto evidencia que, aunque existe capacidad de cierre para este sistema, persiste la necesidad de fortalecer mecanismos de prevención, documentación de soluciones definitivas y análisis de patrones repetitivos.

La concentración conjunta de Inclusión Financiera y ENEE resulta significativa, ya que ambos sistemas acumulan 21 incidencias, equivalentes al 37.5% del total. Esta concentración contrasta con la dispersión observada en los demás sistemas, lo cual indica que la carga de soporte no se distribuye de forma homogénea. En consecuencia, el modelo propuesto de gestión de incidencias debe considerar mecanismos diferenciados para los sistemas con mayor recurrencia, especialmente aquellos vinculados a procesos regulatorios, integraciones externas o actividades críticas de las áreas de Negocios y Operaciones.

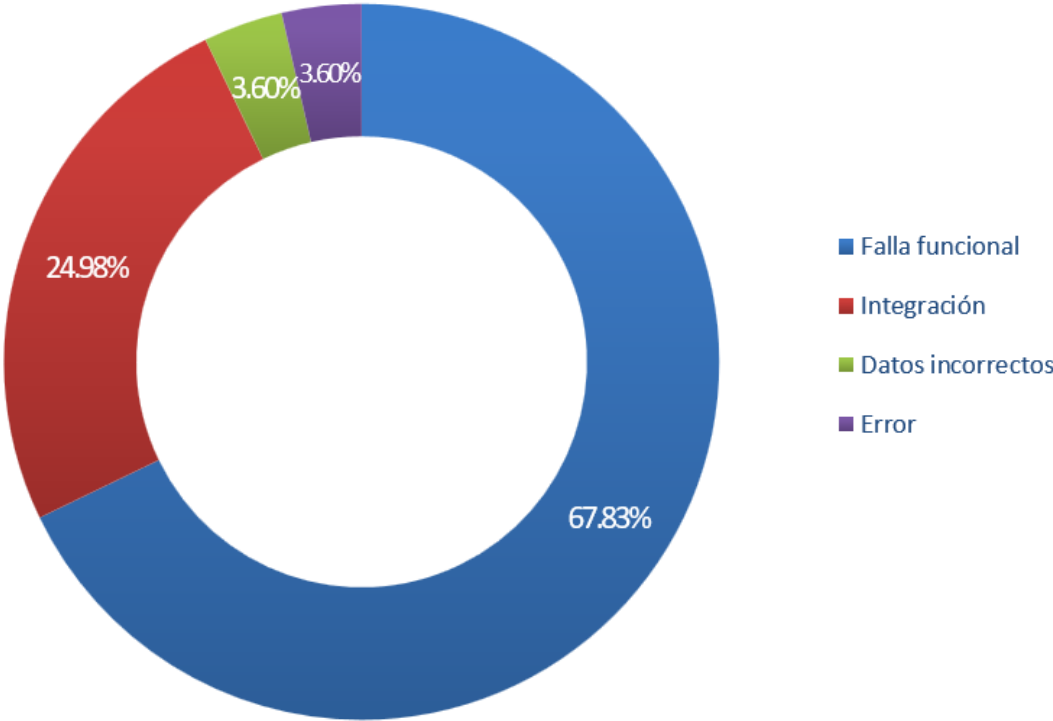
Desde la perspectiva de COBIT 2019, los sistemas con impacto potencial sobre cumplimiento, continuidad operativa o riesgo tecnológico deben ser objeto de seguimiento y control prioritario. En este sentido, los casos asociados a Inclusión Financiera requieren especial atención, debido a su relación con reportes regulatorios ante la CNBS. Por tanto, este análisis contribuye al cumplimiento del Objetivo 1, al caracterizar la situación actual de la gestión de incidencias por sistema afectado, y al Objetivo 3, al clasificar y cuantificar las incidencias según los sistemas involucrados.

4.2.2.4.DISTRIBUCIÓN POR TIPO DE INCIDENCIA

En cuanto a la clasificación por tipo de incidencia, los datos de la Matriz Documental revelan que el universo de 56 casos se distribuye en cuatro categorías principales. Las fallas funcionales constituyen el tipo predominante, con 38 incidencias, equivalentes al 67.9% del total. Las incidencias de integración representan el segundo tipo más frecuente, con 14 casos, equivalentes al 25.0%. En menor proporción se ubican las categorías de datos incorrectos y error, con 2 incidencias cada una, equivalentes al 3.6% por categoría.

En conjunto, las fallas funcionales y las incidencias de integración concentran 52 incidencias, lo que representa el 92.9% de la totalidad de los casos registrados durante el año 2025. Este resultado evidencia que la mayor parte de la problemática documentada se concentra en dos tipos de afectación: por un lado, fallas relacionadas con el funcionamiento esperado de los sistemas; y por otro, fallas asociadas a la comunicación o intercambio de información entre aplicaciones.

Gráfico 39. Distribución de incidencias por tipo, año 2025.



Fuente: Elaboración propia con base en la Matriz Documental de Incidencias.

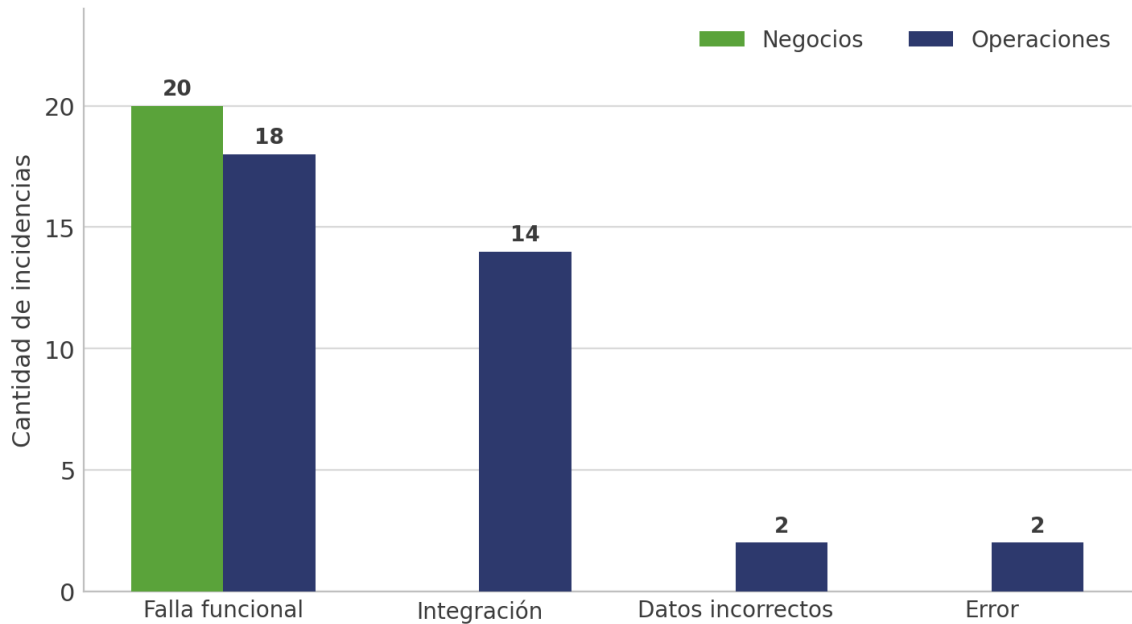
La marcada predominancia de las fallas funcionales indica que la mayor parte de los problemas reportados afectan directamente la operatividad de las funciones de negocio soportadas por los sistemas de software. Este tipo de incidencia puede manifestarse cuando el sistema no permite ejecutar una operación esperada, genera resultados incompletos, impide procesar información o limita el uso normal de una funcionalidad requerida por las áreas usuarias.

Al desagregar los datos por área funcional, se observa un comportamiento diferenciado. El área de Negocios registra el 100% de sus 20 incidencias bajo la categoría de falla funcional, sin presentar incidencias de integración, datos incorrectos o error. Este comportamiento se relaciona

principalmente con los sistemas utilizados por dicha área, especialmente aquellos asociados a reportes, servicios al cliente o procesos comerciales.

En contraste, el área de Operaciones presenta una distribución más diversificada: 18 fallas funcionales, equivalentes al 50.0% de sus casos; 14 incidencias de integración, equivalentes al 38.9%; 2 incidencias de datos incorrectos, equivalentes al 5.6%; y 2 incidencias de tipo error, equivalentes al 5.6%. Esta composición refleja que Operaciones no solo enfrenta problemas funcionales internos, sino también fallas asociadas a integraciones con sistemas externos o plataformas de intercambio de información.

Gráfico 40. Tipo de incidencia según área funcional, año 2025.



Fuente: Elaboración propia con base en la Matriz Documental de Incidencias.

Las incidencias de integración, que representan el 25.0% del total y se concentran completamente en el área de Operaciones, requieren una lectura particular. Este tipo de incidencia apunta hacia fallas en la comunicación entre sistemas, interrupciones en el intercambio de datos o problemas en procesos conectados con entidades externas. En el contexto bancario, este tipo de fallas puede tener implicaciones operativas relevantes, debido a que muchas operaciones dependen de la correcta interacción entre aplicaciones internas, sistemas de recaudación, servicios de pago o plataformas de terceros.

Un aspecto relevante es que 13 de las 14 incidencias de integración fueron resueltas

durante el período analizado, lo que representa una tasa de resolución del 92.9% para este tipo de incidencia. Este resultado contrasta con la tasa global de resolución del conjunto de datos y sugiere que las incidencias de integración, aunque frecuentes, cuentan con mecanismos de atención más efectivos que otros tipos de fallas, particularmente las fallas funcionales recurrentes.

La distinción entre fallas funcionales e incidencias de integración resulta importante desde el punto de vista operativo, ya que cada tipo de incidencia requiere rutas de atención distintas. Las fallas funcionales suelen requerir intervención del equipo de soporte aplicativo o del área de Desarrollo, mientras que las incidencias de integración pueden demandar coordinación entre equipos técnicos, áreas usuarias y, en algunos casos, proveedores o entidades externas.

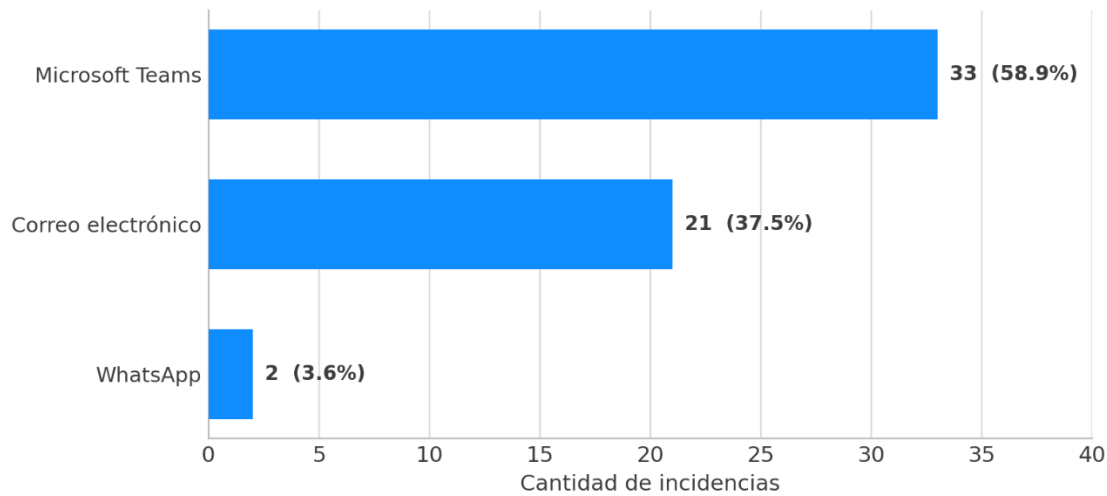
Desde la perspectiva de ITIL 4, esta clasificación permite diseñar modelos de incidente diferenciados según la naturaleza de la falla. Esto significa que el proceso formal propuesto no debe tratar todas las incidencias de la misma manera, sino definir rutas de registro, priorización, escalamiento y resolución según el tipo de afectación reportada. En ese sentido, los resultados de esta sección contribuyen al cumplimiento del Objetivo 3, al clasificar y cuantificar las incidencias de software según su tipo, y aportan insumos para el diseño del flujo formal de gestión de incidencias basado en ITIL 4.

4.2.2.5. DISTRIBUCIÓN POR MEDIO DE REPORTE Y TIPO DE REGISTRO

En relación con el medio de reporte utilizado, los datos de la Matriz Documental indican que Microsoft Teams constituye el canal predominante, con 33 incidencias reportadas a través de este medio, equivalentes al 58.9% del total. El correo electrónico ocupa el segundo lugar, con 21 incidencias, correspondientes al 37.5%, mientras que WhatsApp registra únicamente 2 casos, equivalentes al 3.6%.

La coexistencia de tres canales de reporte diferentes evidencias que, durante el año 2025, las incidencias de software fueron comunicadas mediante mecanismos diversos y no centralizados. Si bien estos medios permiten establecer comunicación entre los usuarios y las áreas técnicas, no todos generan el mismo nivel de trazabilidad, estructura documental ni facilidad para el seguimiento posterior del caso.

Gráfico 41. Distribución de incidencias por medio de reporte, año 2025.



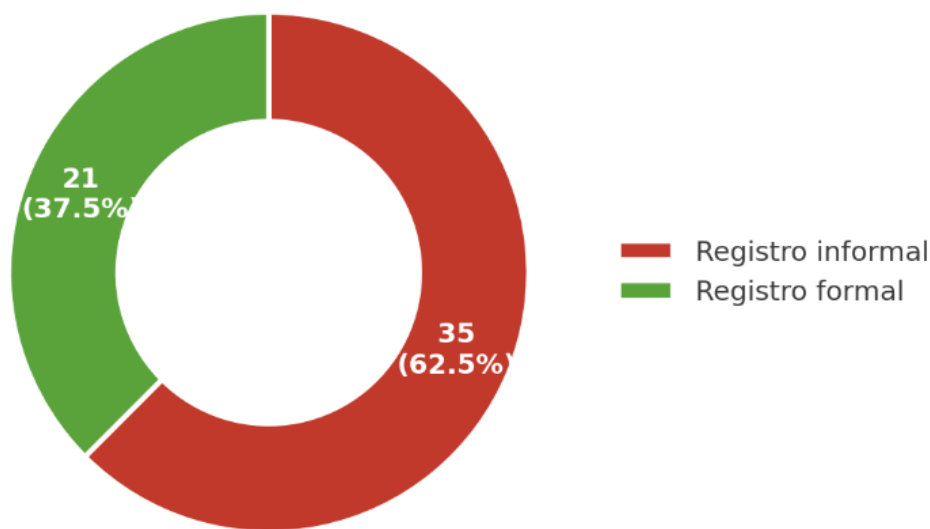
Fuente: Elaboración propia con base en la Matriz Documental de Incidencias.

Respecto al tipo de registro, la Matriz Documental establece que 35 de las 56 incidencias, equivalentes al 62.5%, fueron gestionadas mediante registro informal. Por otra parte, únicamente 21 incidencias, equivalentes al 37.5%, cuentan con registro formal.

El medio de reporte tiene un impacto directo en la calidad del control. El correo puede conservar evidencia básica, pero no necesariamente permite categorizar, medir SLA o asignar estados de manera estandarizada. Teams y WhatsApp facilitan comunicación rápida, pero pueden dispersar información crítica si no se integran a un registro formal. En el contexto de COBIT 2019, esta dispersión limita la capacidad de demostrar control, desempeño y responsabilidad sobre los servicios de TI (ISACA, 2018). La experiencia de Banco Davivienda es especialmente cercana a este hallazgo, ya que su investigación identificó desorganización en el registro, seguimiento y documentación de solicitudes cuando la herramienta ServiceDesk no estaba alineada con ITIL V.4 Almendarez Rodríguez & Cuellar Varela (2024).

El banco debe diferenciar entre canal de comunicación y canal oficial de gestión. Aunque se usen medios ágiles para coordinación, el registro formal debe realizarse en una herramienta centralizada. Esta decisión reduciría riesgo operativo, fortalecería el control documental y permitiría construir indicadores confiables de desempeño (Comisión Nacional de Bancos y Seguros, 2022).

Gráfico 42. Tipo de registro de las incidencias: formal vs. informal, año 2025.



Fuente: Elaboración propia con base en la Matriz Documental de Incidencias.

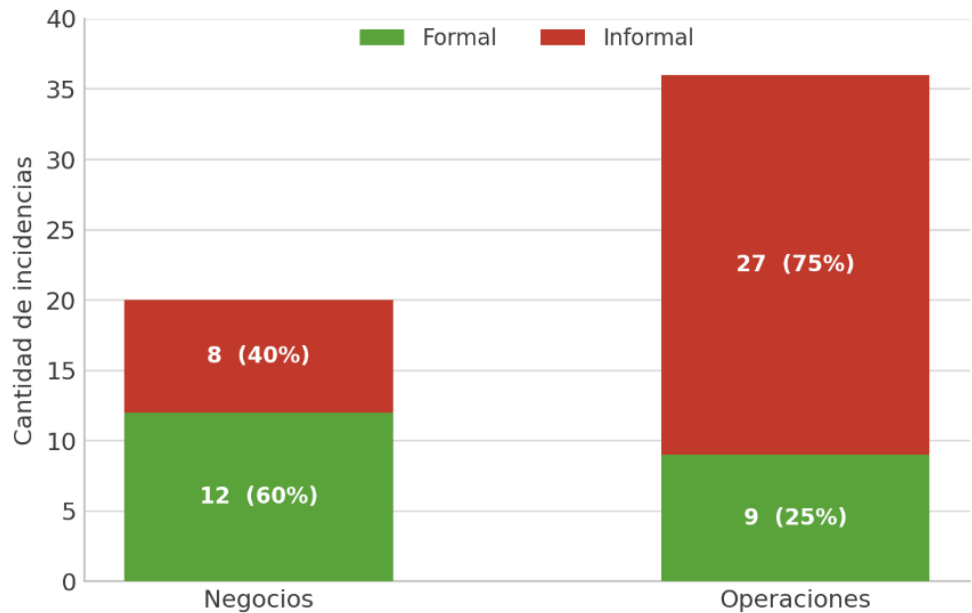
Al desagregar el tipo de registro por área funcional, se identifican diferencias relevantes. El área de Negocios presenta una mayor proporción de registros formales, con 12 incidencias formales de 20 casos, equivalentes al 60.0%. Las 8 incidencias restantes, equivalentes al 40.0%, fueron gestionadas mediante registros informales.

En contraste, el área de Operaciones presenta una mayor dependencia de registros informales. De sus 36 incidencias, 27 fueron informales, equivalentes al 75.0%, mientras que solo 9 casos, equivalentes al 25.0%, cuentan con registro formal. Esta diferencia evidencia que la informalidad en el registro se concentra principalmente en Operaciones, área que además registra el mayor volumen de incidencias durante el período analizado.

Este es uno de los hallazgos más relevantes del estudio. La informalidad en el registro no significa necesariamente ausencia de atención, pero sí limita la capacidad del banco para demostrar control sobre el proceso. Desde una perspectiva financiera, una incidencia informal puede generar costos invisibles: reprocesos, tiempos muertos, interrupciones no medidas y decisiones sin respaldo histórico. La normativa de gestión de tecnologías de información exige a las instituciones supervisadas contar con procesos documentados y controles sobre disponibilidad, integridad y continuidad (Comisión Nacional de Bancos y Seguros, 2022). Esto coincide con Martínez Dubón

y Andrade Suazo (2021), quienes encontraron que sin reportes y registros adecuados el equipo de soporte desconoce el volumen real de requerimientos recibidos, lo que limita la medición y la toma de decisiones.

Gráfico 43. Tipo de registro según área funcional, año 2025.



Fuente: Elaboración propia con base en la Matriz Documental de Incidencias.

La predominancia del registro informal tiene implicaciones directas sobre la trazabilidad del proceso. Cuando una incidencia es reportada por canales de mensajería instantánea, la información puede quedar dispersa, depender del seguimiento individual del receptor y carecer de campos estandarizados como prioridad, responsable asignado, estado, fecha de atención, fecha de resolución o evidencia de cierre. En consecuencia, se dificulta la generación de indicadores confiables, la auditoría del proceso y la identificación de patrones de comportamiento a lo largo del tiempo.

Este resultado demuestra que la informalidad no se distribuye de la misma manera entre áreas. Operaciones concentra mayor volumen de incidencias y mayor proporción de registros informales, lo cual incrementa la exposición operativa porque esta área suele estar vinculada a procesos transaccionales, conciliaciones, pagos y actividades de continuidad diaria. Desde el enfoque de gestión de riesgos, las áreas con mayor criticidad operativa requieren controles más estrictos y evidencia más completa (Organización Internacional de Normalización, 2018;

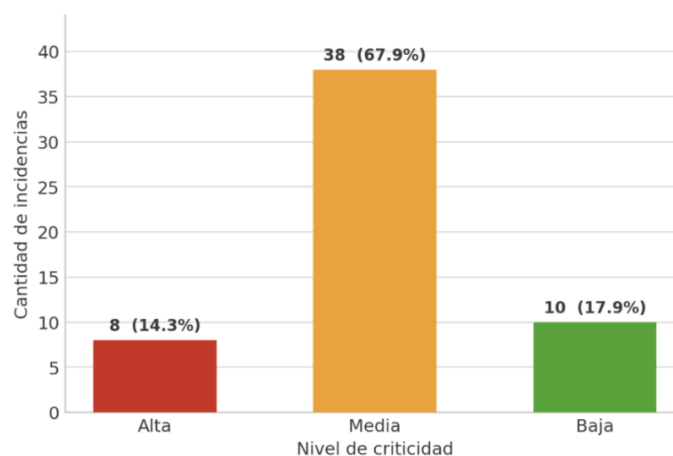
Comisión Nacional de Bancos y Seguros, 2022). Desde la experiencia de Banco Davivienda, la reingeniería del catálogo de servicios, la definición de SLA y la generación de reportes fueron propuestas como acciones necesarias para ordenar la atención y mejorar la percepción del cliente interno. Esta subsección cumple de manera directa con el Objetivo 4 de la investigación, al determinar que el 62.5% de las incidencias de software registradas durante el año 2025 fueron gestionadas sin registro formal. Asimismo, aporta al Objetivo 1, ya que la trazabilidad y el control operativo del proceso dependen de la existencia de registros estructurados, verificables y auditables.

Desde la perspectiva de ITIL 4, la formalización del registro no implica necesariamente crear procesos complejos, sino establecer mecanismos simples, prácticos y consistentes que permitan registrar, clasificar, asignar, monitorear y cerrar cada incidencia de manera controlada. Por ello, un sistema de tickets o portal de autoservicio permitiría reducir la dispersión de canales, mejorar la trazabilidad y fortalecer la medición del desempeño del proceso de gestión de incidencias.

4.2.2.6. DISTRIBUCIÓN POR NIVEL DE CRITICIDAD

Los datos obtenidos respecto al nivel de criticidad asignado a las 56 incidencias registradas revelan una concentración importante en la categoría de criticidad media. Esta categoría agrupa 38 incidencias, equivalentes al 67.9% del total. Le sigue la criticidad baja, con 10 incidencias, equivalentes al 17.9%, mientras que la criticidad alta registra 8 incidencias, correspondientes al 14.3% del universo analizado.

Gráfico 44. Distribución de incidencias por nivel de criticidad, año 2025.



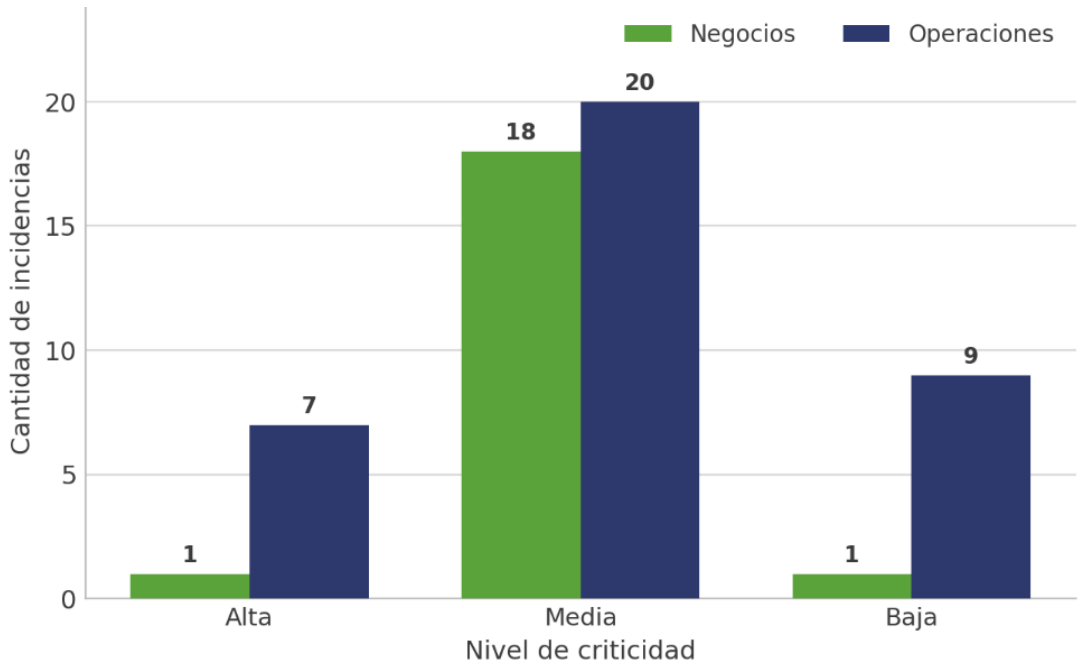
Fuente: Elaboración propia con base en la Matriz Documental de Incidencias.

Al realizar el cruce entre área funcional y nivel de criticidad, se identifican diferencias relevantes. El área de Negocios registra 18 de sus 20 incidencias bajo criticidad media, equivalentes al 90.0%. Además, presenta 1 incidencia de criticidad alta y 1 incidencia de criticidad baja, equivalentes al 5.0% cada una.

Por su parte, el área de Operaciones presenta una distribución más diversificada: 7 incidencias de criticidad alta, equivalentes al 19.4% de sus casos; 20 incidencias de criticidad media, equivalentes al 55.6%; y 9 incidencias de criticidad baja, equivalentes al 25.0%.

La criticidad es un elemento clave para conectar el análisis técnico con el negocio bancario. Una incidencia no debe clasificarse únicamente por la dificultad técnica, sino por el impacto que genera sobre procesos, usuarios, clientes, cumplimiento regulatorio y continuidad operativa. ISO 31000 plantea que la gestión del riesgo debe considerar el efecto de la incertidumbre sobre los objetivos (Organización Internacional de Normalización, 2018). Bajo esa lógica, la criticidad de una incidencia debe reflejar su posible efecto sobre los objetivos operativos del banco. Moncada Martínez y Godoy Godoy (2025) aplicar COBIT 2019 en la UNAH, evidenciaron que la falta de estandarización, planificación, seguimiento y control afecta la eficiencia y la gobernanza tecnológica, lo cual respalda la necesidad de clasificar las incidencias con criterios más robustos

Gráfico 45. Nivel de criticidad según área funcional, año 2025.



Fuente: Elaboración propia con base en la Matriz Documental de Incidencias.

La concentración de casos en criticidad media merece especial atención, ya que podría reflejar una tendencia a clasificar la mayoría de las incidencias en un nivel intermedio, aun cuando algunas de ellas se encuentren asociadas a sistemas con impacto operativo o regulatorio relevante. En el caso del área de Negocios, las incidencias del sistema Inclusión Financiera fueron clasificadas como criticidad media, a pesar de estar relacionadas con la generación de reportes vinculados a la Comisión Nacional de Bancos y Seguros (CNBS) y de permanecer sin resolución documentada al cierre del período analizado.

La concentración de casos medios en Negocios podría reflejar una tendencia a clasificar de forma intermedia situaciones que tal vez ameritan mayor revisión. En particular, si algunos casos están vinculados a reportes, atención comercial o procesos que impactan al cliente, clasificarlos como criticidad media podría subestimar su importancia. COBIT 2019 plantea que los criterios de gestión deben responder al valor y al riesgo del negocio, por lo que la criticidad debe validarse con las áreas usuarias (ISACA, 2018). Este enfoque se alinea con Moncada Martínez y Godoy Godoy (2025) quienes vinculan COBIT 2019 con mecanismos de monitoreo, roles definidos y control para asegurar que las decisiones tecnológicas respondan a necesidades institucionales.

La criticidad debe validarse con participación de las áreas de negocio y no ser definida únicamente desde TI. Esto permitiría capturar mejor la afectación real de cada incidencia y evitar que casos sensibles queden sin prioridad suficiente. En el sector financiero, esta práctica ayuda a fortalecer la continuidad operativa y el cumplimiento de controles regulatorios (Comisión Nacional de Bancos y Seguros, 2022)

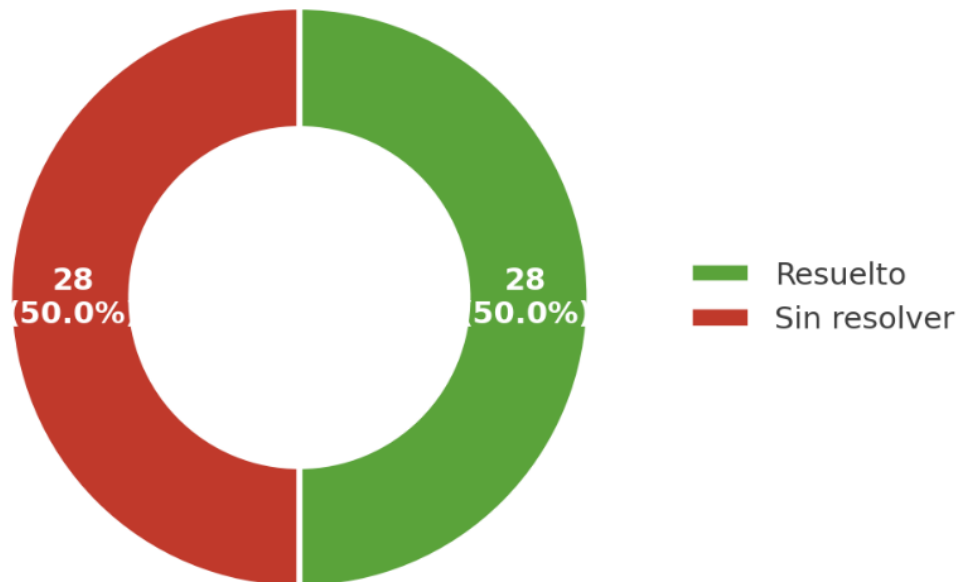
4.2.2.7. ESTADO DE RESOLUCIÓN Y ANÁLISIS DE REINCIDENCIA

El estado de resolución de las incidencias constituye uno de los indicadores más directos para evaluar el desempeño del proceso actual de gestión de incidencias de software. Los resultados de la Matriz Documental revelan que, al cierre del período analizado, 28 de las 56 incidencias se encontraban en estado resuelto, equivalentes al 50.0%, mientras que las 28 incidencias restantes permanecían en estado sin resolver, representando también el 50.0% del total.

Este resultado evidencia que la mitad de las incidencias documentadas durante el año 2025 no cuenta con cierre formal registrado, lo cual limita la trazabilidad del proceso y dificulta confirmar si el servicio fue restaurado, si el usuario validó la solución o si el caso requería

seguimiento adicional.

Gráfico 46. Estado de resolución de las incidencias, año 2025.

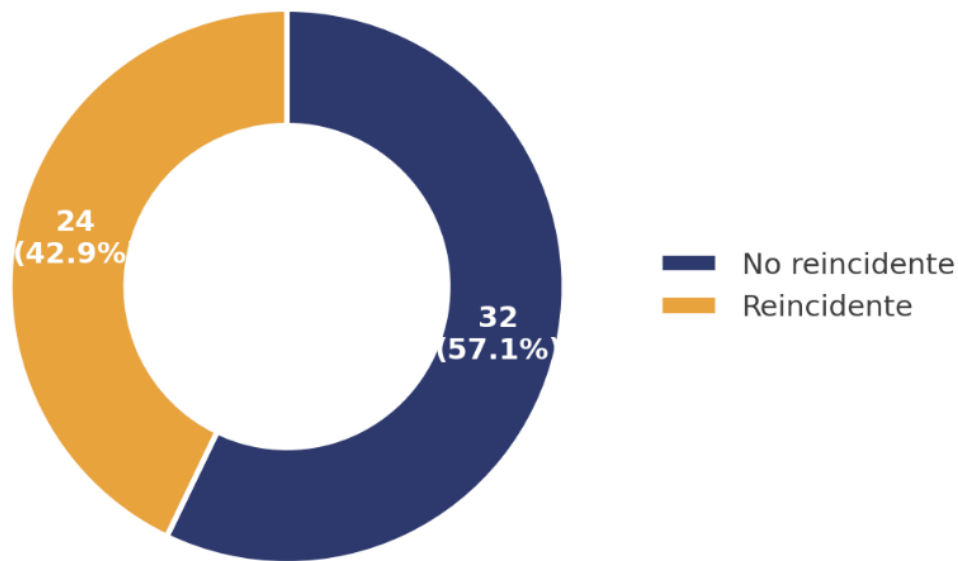


Fuente: Elaboración propia con base en la Matriz Documental de Incidencias.

Al analizar el estado de resolución por área funcional, se identifican diferencias significativas. El área de Operaciones muestra una mayor capacidad de cierre, con 27 de sus 36 incidencias resueltas, equivalentes al 75.0%, y 9 incidencias sin resolver, equivalentes al 25.0%. En contraste, el área de Negocios registra únicamente 1 incidencia resuelta de 20 casos, equivalente al 5.0%, mientras que 19 incidencias permanecen sin resolver, equivalentes al 95.0%.

Este resultado representa una alerta de control. Un 50.0% de incidencias sin cierre documentado no necesariamente implica que todas continúen afectando la operación, pero sí impide demostrar que fueron corregidas, validadas y cerradas. AXELOS (2019) ubica el cierre como parte del ciclo de vida de la atención de incidencias, mientras que ISO/IEC 20000-1 exige que los servicios se gestionen mediante controles y mejora continua (Organización Internacional de Normalización, 2018). Por tanto, cerrar documentalmente no es una formalidad administrativa, sino una evidencia de control. En estudios de mesa de servicio, el cierre documentado no es un trámite menor: en Banco Davivienda se identificó la necesidad de contar con estadísticas claras y documentación ordenada para mejorar la gestión y percepción del servicio (Almendarez Rodríguez & Cuéllar Varela, 2024).

Gráfico 47. Condición de reincidencia de las incidencias, año 2025.

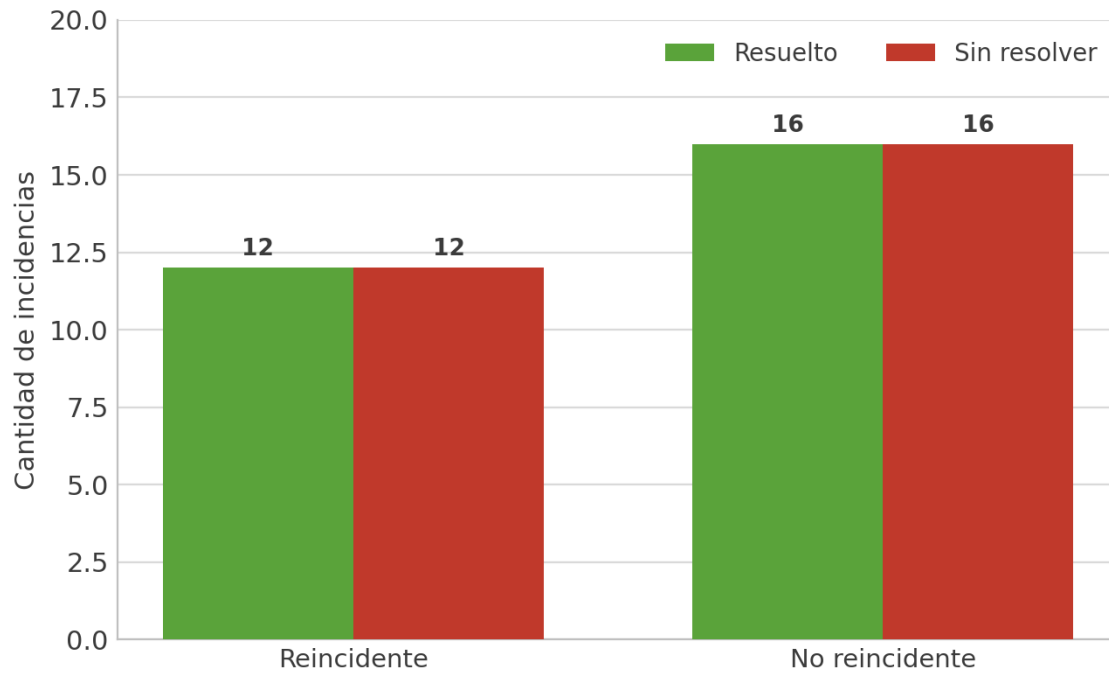


Fuente: Elaboración propia con base en la Matriz Documental de Incidencias.

El análisis combinado del estado de resolución y la reincidencia permite profundizar en el comportamiento del proceso. Del total de 24 incidencias reincidentes, 12 fueron resueltas y 12 permanecen sin resolver. Asimismo, de las 32 incidencias no reincidentes, 16 fueron resueltas y 16 permanecen sin resolver. Esta distribución muestra que la condición de reincidencia, por sí sola, no determina la probabilidad de cierre, ya que tanto las incidencias reincidentes como las no reincidentes presentan una proporción similar de casos resueltos y sin resolver.

La tasa de reincidencia del 42.9% es uno de los hallazgos más fuertes de la investigación. Este porcentaje indica que una parte considerable de los casos no corresponde a eventos aislados, sino a fallas que se repiten o que no han sido corregidas desde su causa raíz. ITIL 4 establece que la gestión de problemas se enfoca en reducir la probabilidad y el impacto de incidentes mediante la identificación de causas y soluciones permanentes (AXELOS, 2019). En términos de productividad, cada reincidencia obliga al usuario a volver a reportar, al equipo de TI a volver a analizar y al negocio a convivir con interrupciones repetidas. La investigación de Martínez Dubón y Andrade Suazo (2021) también incluyó la gestión de problemas como parte del diseño de Service Desk basado en ITIL4, lo cual respalda que la reincidencia no debe tratarse solo como repetición de tickets, sino como señal de causas raíz no resueltas.

Gráfico 48. Estado de resolución según condición de reincidencia, año 2025.



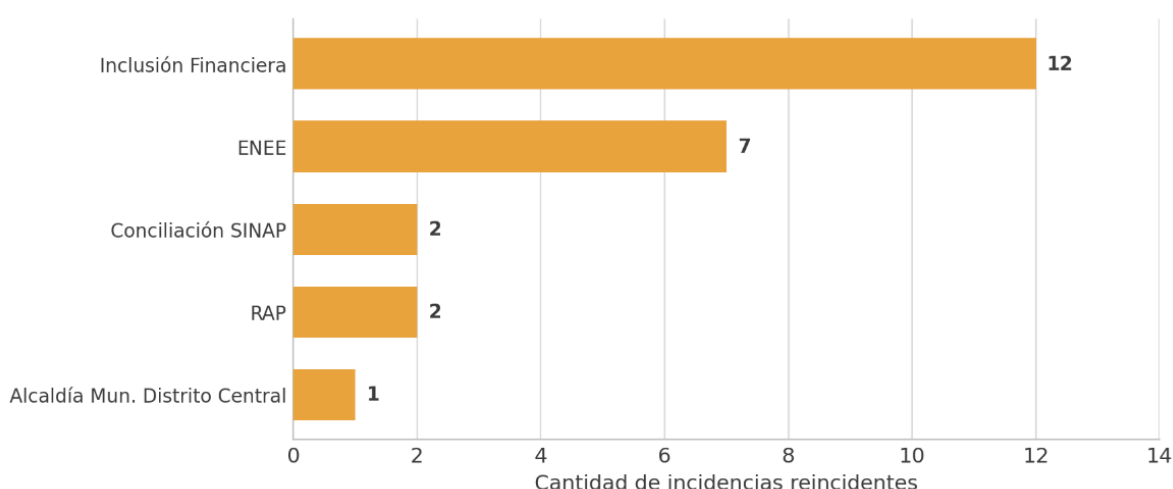
Fuente: Elaboración propia con base en la Matriz Documental de Incidencias.

La concentración de la reincidencia en sistemas específicos también constituye un hallazgo relevante. El sistema Inclusión Financiera acumula 12 incidencias reincidentes, todas en estado sin resolver, convirtiéndose en el principal foco de incidencias recurrentes sin cierre documentado. El sistema ENEE registra 7 incidencias reincidentes, aunque en este caso todas fueron resueltas. Los sistemas Conciliación SINAP y RAP registran 2 casos reincidentes cada uno, mientras que Alcaldía Municipal del Distrito Central registra 1 caso reincidente.

Este comportamiento demuestra que el problema no se limita a la reincidencia, sino también al cierre del ciclo de vida de la incidencia. Que una incidencia sea recurrente no garantiza mayor seguimiento, y que no sea recurrente tampoco asegura cierre formal. Desde la perspectiva de ITSM, esto refleja una brecha de madurez porque el proceso no diferencia con suficiente fuerza entre atender, resolver, validar y cerrar. La mejora del proceso requiere controles de estado y criterios claros de transición entre etapas (Organización Internacional de Normalización, 2018). Esta separación entre atención, resolución y cierre es coherente con la lógica aplicada en estudios previos de Service Desk, donde la formalización del proceso busca generar reportes, mejorar seguimiento y apoyar la toma de decisiones (Martínez Dubón & Andrade Suazo , 2021).

El modelo debe separar claramente tres controles: resolución técnica, validación del usuario y cierre documental. Además, las incidencias reincidentes deberían activar revisión de problema, mientras que las incidencias no reincidentes deberían cerrarse con evidencia mínima. Esta separación fortalece trazabilidad, aprendizaje y control operativo (AXELOS, 2019).

Gráfico 49. Sistemas con mayor número de incidencias reincidentes, año 2025.



Fuente: Elaboración propia con base en la Matriz Documental de Incidencias.

El caso de Inclusión Financiera requiere especial atención, ya que sus incidencias se repiten durante el año, permanecen sin resolución documentada y están relacionadas con la generación de reportes vinculados a la Comisión Nacional de Bancos y Seguros (CNBS). Esta condición representa un riesgo operativo y regulatorio relevante, debido a que la falta de cierre formal impide evidenciar que la falla fue corregida de manera definitiva.

Por su parte, el caso de ENEE muestra una dinámica distinta: las incidencias fueron resueltas, pero presentan recurrencia. Esto indica que el proceso puede estar logrando restaurar la operación, pero no necesariamente eliminar la causa que origina la repetición de la falla. Por ello, ambos sistemas reflejan necesidades diferentes: Inclusión Financiera requiere gestión prioritaria de cierre y escalamiento, mientras que ENEE requiere análisis de causa raíz y prevención de recurrencia.

Desde la perspectiva de ITIL 4, este resultado evidencia la necesidad de articular la gestión de incidencias con la gestión de problemas. La gestión de incidencias permite restaurar el servicio en el menor tiempo posible, pero la gestión de problemas permite investigar y eliminar

las causas raíz de los incidentes recurrentes. En este sentido, la reincidencia identificada en sistemas como Inclusión Financiera, ENEE, RAP y Conciliación SINAP justifica la incorporación de mecanismos de análisis de causa raíz dentro del modelo propuesto.

Este resultado permite profundizar el análisis de causa raíz. Inclusión Financiera representa una situación crítica porque combina recurrencia, ausencia de cierre y relación con reportes a la CNBS. ENEE presenta un comportamiento distinto: reincidencia, pero con casos resueltos. La Comisión Nacional de Bancos y Seguros (2022) refuerza la importancia de gestionar la continuidad y los riesgos tecnológicos en instituciones supervisadas. Por ello, no basta con contar incidencias; es necesario evaluar criticidad del sistema, estado, recurrencia, impacto regulatorio y continuidad del servicio.

No todos los sistemas reincidentes requieren la misma respuesta. Inclusión Financiera necesita cierre prioritario, escalamiento y revisión de riesgo regulatorio. ENEE requiere análisis de causa raíz para evitar repetición. Otros sistemas con menor volumen deben mantenerse bajo monitoreo. Esta clasificación permitiría asignar recursos de Desarrollo de forma más estratégica

4.2.2.8. ANÁLISIS INTERPRETATIVO DE POSIBLES CAUSAS RAÍZ POR SISTEMA

Con base en los resultados obtenidos en el análisis de reincidencia, se considera necesario profundizar en los sistemas que presentaron una mayor repetición de incidencias durante el período evaluado. Este análisis permite pasar de una lectura únicamente cuantitativa de los casos reincidentes hacia una interpretación más estratégica, orientada a identificar posibles causas raíz, implicaciones operativas y acciones de mejora. La reincidencia no debe entenderse solamente como la repetición de una falla, sino como una señal de que la solución aplicada pudo haber sido temporal, incompleta o insuficiente para eliminar el origen del problema.

Desde la perspectiva de ITIL 4, la gestión de incidencias busca restaurar la operación normal del servicio en el menor tiempo posible; sin embargo, cuando los eventos se repiten en un mismo sistema, resulta necesario complementar esta práctica con la gestión de problemas. Esto permitiría identificar patrones, analizar causas comunes y definir acciones preventivas que reduzcan la probabilidad de nuevas ocurrencias. En el contexto de Banco Ficensa, este análisis es relevante porque las incidencias reincidentes pueden generar reprocesos, pérdida de productividad, mayor carga para el área de Desarrollo y afectación en la continuidad operativa de procesos críticos de Negocios y Operaciones.

Tabla 22: Análisis interpretativo de posibles causas raíz por sistema

Sistema	Patrón identificado	Posible causa raíz	Implicación operativa	Acción sugerida
Inclusión Financiera	Alta reincidencia y casos pendientes	Fallas persistentes en lógica de negocio, reportes, validaciones o parametrizaciones	Riesgo de reprocesos, atrasos operativos y afectación a usuarios internos	Abrir análisis de problema, documentar causa raíz y definir plan correctivo
ENEE	Casos reincidentes registrados como resueltos	Soluciones temporales, inestabilidad en integración o eventos asociados a una misma plataforma tecnológica	Incremento de carga operativa y necesidad de seguimiento manual repetitivo	Validar si las soluciones aplicadas eliminaron la causa raíz y aplicar monitoreo posterior al cierre
RAP	Reincidencias asociadas a procesos específicos	Dependencias de integración, reglas de validación o inconsistencias en datos procesados	Posibles retrasos en procesos operativos y necesidad de reprocesamiento	Revisar reglas funcionales, pruebas de validación y evidencia de cierre
Conciliación SINAP	Repetición de fallas en actividades de conciliación	Errores en integración, validación de información o controles posteriores al procesamiento	Riesgo de inconsistencias operativas y mayor esfuerzo de verificación	Fortalecer pruebas funcionales, controles de conciliación y seguimiento preventivo
Alcaldía Municipal del Distrito Central	Reincidencias menores, pero relacionadas con procesos operativos específicos	Dependencia de procesos externos, integración o validaciones incompletas	Posibles demoras en la atención de solicitudes internas	Documentar patrón de falla y evaluar acciones preventivas
Otros sistemas afectados	Repetición ocasional de incidencias	Falta de categorización estandarizada, documentación incompleta o ausencia de análisis histórico	Dificultad para identificar tendencias y priorizar mejoras	Fortalecer el registro formal, clasificación y análisis periódico de tendencia

Fuente: Elaboración propia con base en la Matriz Documental de Incidencias de Software, año 2025.

La tabla anterior evidencia que las incidencias reincidentes no se explican únicamente por fallas técnicas aisladas, sino por posibles debilidades en el diagnóstico, documentación, validación y cierre definitivo de los casos. En este sentido, los sistemas con mayor reincidencia deben ser tratados como candidatos prioritarios para análisis de causa raíz, debido a que concentran eventos repetitivos que pueden afectar la productividad de los usuarios y la estabilidad operativa de los servicios tecnológicos. Por tanto, la propuesta de gestión de incidencias debe incorporar mecanismos de identificación de casos recurrentes, escalamiento hacia gestión de problemas y seguimiento posterior al cierre, con el fin de reducir la repetición de fallas y fortalecer la mejora continua del servicio.

4.2.2.9. ANÁLISIS DE TIEMPOS DE ATENCIÓN Y RESOLUCIÓN

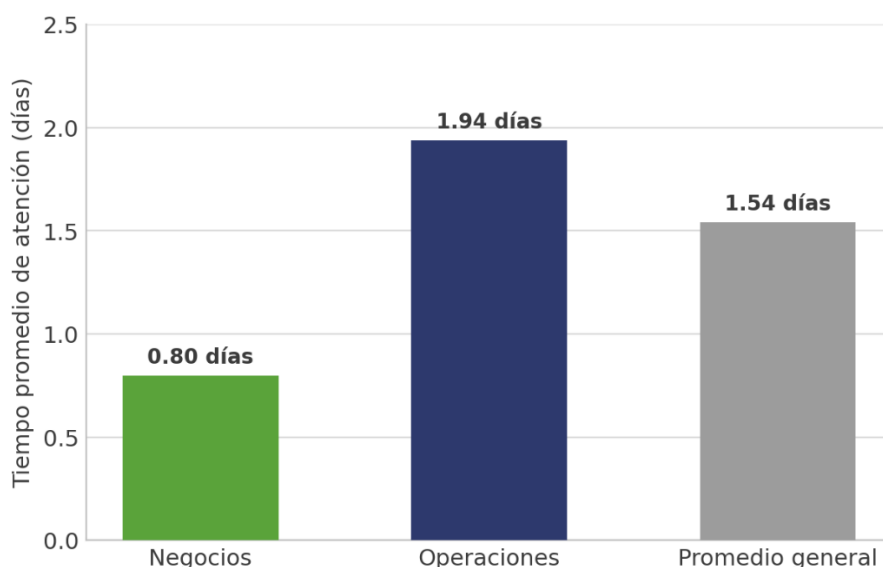
De acuerdo con los resultados obtenidos en la Matriz Documental, el tiempo promedio de atención de las 56 incidencias registradas durante el año 2025 fue de 1.54 días, con un valor mínimo de 0 días y un valor máximo de 20 días. Asimismo, la desviación estándar fue de 2.95 días, lo que refleja variabilidad en los tiempos de primera atención entre los casos analizados.

Un dato relevante es que 28 de las 56 incidencias, equivalentes al 50.0%, fueron atendidas el mismo día de su reporte. Esto indica que en la mitad de los casos existió una respuesta inicial inmediata. Sin embargo, la existencia de un caso con tiempo de atención de hasta 20 días evidencia que el proceso no cuenta con un comportamiento completamente uniforme, lo cual puede estar relacionado con la ausencia de tiempos máximos formalmente definidos para la primera respuesta.

Al analizar el tiempo de atención por área funcional, se identifican diferencias importantes. El área de Negocios registra un tiempo promedio de atención de 0.80 días, con 13 de sus 20 incidencias atendidas el mismo día del reporte, equivalentes al 65.0%. Por su parte, el área de Operaciones presenta un tiempo promedio de atención de 1.94 días, con 15 de sus 36 incidencias atendidas el mismo día, equivalentes al 41.7%.

Este resultado muestra que Negocios tiene una atención inicial más rápida que Operaciones. No obstante, dicha rapidez no se traduce necesariamente en resolución efectiva, ya que Negocios presenta una baja tasa de cierre formal de incidencias. Por tanto, el análisis evidencia una diferencia importante entre atender inicialmente una incidencia y resolverla de manera documentada.

Gráfico 50. Tiempo promedio de atención por área funcional, año 2025.



Fuente: Elaboración propia con base en la Matriz Documental de Incidencias.

En cuanto al tiempo de resolución, el análisis se realizó únicamente sobre las 28 incidencias que cuentan con fecha de cierre, ya que las otras 28 permanecen en estado sin resolver y no disponen de información suficiente para calcular este indicador. Sobre este subconjunto, el tiempo promedio de resolución fue de 8.57 días, con un valor mínimo de 0 días, un valor máximo de 43 días y una desviación estándar de 10.98 días.

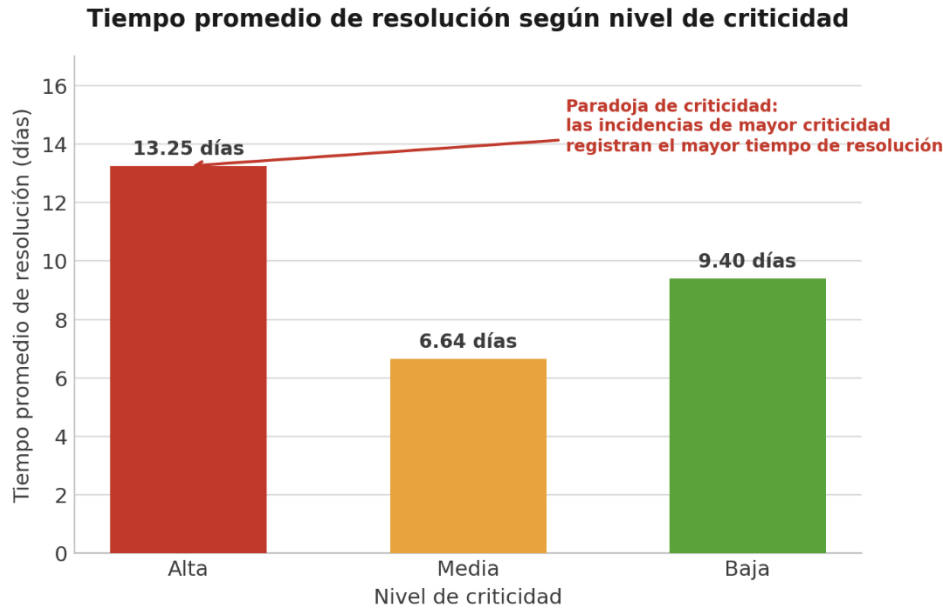
La mediana del tiempo de resolución fue de 4.5 días, lo que indica que la mitad de los casos resueltos se cerró en menos de una semana. Además, 15 de las 28 incidencias resueltas, equivalentes al 53.6%, fueron cerradas en un plazo igual o inferior a 5 días. Sin embargo, la diferencia entre la media y la mediana muestra que existen casos con tiempos de resolución prolongados que elevan el promedio general.

Entre los casos con mayor tiempo de resolución se identifican incidencias asociadas a los sistemas AMDC, con 43 días; Alcaldía Municipal del Distrito Central, con 30 días; ENEE, con 30 días; Matrícula Vehicular, con 26 días; y otro caso de ENEE, con 20 días. Estos valores evidencian la necesidad de establecer mecanismos de escalamiento cuando una incidencia supera los tiempos esperados de resolución.

El promedio general puede parecer manejable, pero la existencia de valores extremos refleja variabilidad del proceso. Desde el punto de vista financiero y operativo, una atención inicial

tardía puede retrasar correcciones, prolongar el uso de soluciones manuales y aumentar el costo indirecto de la incidencia. Las métricas de gestión de incidentes recomiendan no depender únicamente del promedio, sino revisar máximos, desviaciones, cumplimiento de SLA y tiempos por criticidad (ManageEngine, 2024). La necesidad de medir tiempos y compromisos de atención se observa también en el estudio de Banco Davivienda, donde se propuso definir SLA, monitorear su cumplimiento y generar reportes para elevar la calidad de la mesa de servicio (Almendarez Rodríguez & Cuéllar Varela, 2024).

Gráfico 51. Tiempo promedio de resolución según nivel de criticidad, año 2025.



Fuente: Elaboración propia con base en la Matriz Documental de Incidencias.

Debe considerarse que el cálculo del tiempo promedio de resolución se basa únicamente en las incidencias resueltas. Por tanto, este indicador no refleja completamente la situación de las incidencias que permanecen abiertas. Si se incorporara la carga pendiente de resolución, el desempeño general del proceso podría mostrar una situación más crítica en términos de cierre y control operativo. El análisis de la antigüedad de las incidencias abiertas confirma esta situación, los casos sin resolver con fecha verificable acumulaban una antigüedad promedio de 193 días al cierre del período, muy superior a los 8.57 días de resolución de los casos cerrados. Esto demuestra que el desempeño real del proceso es considerablemente más crítico de lo que sugiere el MTTR calculado únicamente sobre incidencias resueltas.

En el contexto de la presente investigación, este análisis da cumplimiento directo al Objetivo 2, orientado a calcular el tiempo promedio de atención y resolución de las incidencias de software registradas durante el año 2025. Asimismo, aporta información relevante para el Objetivo 5, ya que los tiempos de atención y resolución constituyen indicadores clave de desempeño para evaluar la eficiencia del proceso de gestión de incidencias.

Desde la perspectiva de ITIL 4, los tiempos de primera atención y resolución deben formar parte de los acuerdos de nivel de servicio y de los mecanismos de medición del proceso. En este sentido, la dispersión observada en los tiempos de resolución, junto con el mayor promedio en incidencias de criticidad alta, justifica la necesidad de establecer tiempos objetivos diferenciados por criticidad, reglas de escalamiento automático, responsables asignados y alertas de vencimiento. Estos elementos deben incorporarse en el modelo propuesto para fortalecer la trazabilidad, reducir demoras y mejorar el control operativo de la gestión de incidencias de software en Banco Ficensa.

Este resultado muestra que el desempeño no es homogéneo. Aunque más de la mitad de los casos resueltos se cerró en cinco días o menos, existen incidencias con tiempos prolongados que elevan el promedio general. En banca, un tiempo de resolución de 43 días puede representar una exposición significativa si el sistema afectado soporta procesos críticos, reportes o atención de clientes. ITIL 4 recomienda restaurar el servicio con rapidez, pero también aprender de los incidentes para reducir futuras interrupciones (AXELOS, 2019). Por ello, el MTTR debe interpretarse junto con criticidad, reincidencia y estado de cierre. De manera complementaria, Rodríguez Archaga (2024) destaca que la carencia de indicadores clave de rendimiento limita el control de la atención de incidentes y solicitudes; por ello, el MTTR debe analizarse junto con SLA, reincidencia y criticidad.

4.2.2.10. SÍNTESIS CUANTITATIVA DEL ANÁLISIS DOCUMENTAL

La síntesis cuantitativa del análisis documental evidencia que la gestión de incidencias de software en Banco Ficensa presenta brechas relevantes en materia de trazabilidad, formalización del registro, tiempos de resolución, reincidencia y control operativo. Los datos muestran que las incidencias se presentaron durante todo el año 2025, afectaron diversos sistemas y se concentraron principalmente en el área de Operaciones y en fallas de tipo funcional. Asimismo, el alto porcentaje

de registros informales y la diferencia entre los tiempos de atención inicial y resolución definitiva reflejan la necesidad de fortalecer el proceso mediante un canal único, criterios de criticidad, reglas de escalamiento, seguimiento documentado e indicadores clave de desempeño.

En conjunto, estos resultados constituyen la base para los hallazgos principales de la investigación, los cuales se presentan en la siguiente sección en función de los objetivos específicos planteados.

Tabla 23: Síntesis del análisis documental.

Indicador	Valor
Total de incidencias registradas	56
Período de análisis	Enero – diciembre 2025
Áreas funcionales analizadas	Negocios y Operaciones
Total de sistemas afectados	32
Trimestre con mayor volumen	Q3: julio–septiembre, 18 casos (32.1%)
Área con mayor volumen de incidencias	Operaciones, 36 casos (64.3%)
Sistema con mayor concentración	Inclusión Financiera, 12 casos (21.4%)
Tipo de incidencia predominante	Falla funcional, 38 casos (67.9%)
Criticidad predominante	Media, 38 casos (67.9%)
Canal de reporte más utilizado	Microsoft Teams, 33 casos (58.9%)
Incidencias con registro informal	35 casos (62.5%)
Incidencias con registro formal	21 casos (37.5%)
Incidencias resueltas	28 casos (50.0%)
Incidencias sin resolver	28 casos (50.0%)
Tasa de resolución – Operaciones	75.0% (27 de 36 casos)
Tasa de resolución – Negocios	5.0% (1 de 20 casos)
Tasa de reincidencia global	42.9% (24 casos)
Sistema con mayor reincidencia	Inclusión Financiera, 12 casos reincidentes
Incidencias de alta criticidad sin resolver	4 de 8 casos (50.0%)
Tiempo promedio de atención	1.54 días
Tiempo promedio de resolución	8.57 días, sobre 28 casos resueltos
Tiempo máximo de resolución	43 días, AMDC – Operaciones
Tiempo promedio de resolución – alta criticidad	13.25 días
Tiempo promedio de resolución – media criticidad	6.64 días
Tiempo promedio de resolución – baja criticidad	9.40 días

Tasa de resolución – incidencias de integración	92.9% (13 de 14 casos)
Registro informal – Operaciones	75.0% (27 de 36 casos)
Registro informal – Negocios	40.0% (8 de 20 casos)

Fuente: Elaboración propia con base en la Matriz Documental de Incidencias.



Figura 19. Tablero resumen de indicadores clave del análisis documental, año 2025.

Fuente: Elaboración propia con base en la Matriz Documental de Incidencias.

La lectura integrada de los indicadores permite identificar una serie de brechas relevantes en la gestión actual de incidencias de software en Banco Ficensa. En primer lugar, el análisis confirma que la problemática no es aislada, ya que se registraron incidencias durante todo el año 2025 y se identificaron afectaciones en 32 sistemas distintos. Esto evidencia una demanda recurrente de soporte que requiere un proceso formal, permanente y medible.

En conjunto, los resultados justifican la formulación de un modelo formal de gestión de incidencias de software basado en ITIL 4 y complementado con principios de COBIT 2019. Dicho modelo debe contemplar como mínimo un canal único de registro, criterios objetivos de clasificación y criticidad, acuerdos de nivel de servicio diferenciados, reglas de escalamiento, seguimiento continuo, cierre documentado y mecanismos de análisis de causa raíz para los casos recurrentes.

4.2.3. EVALUACIÓN DE LA CAPACIDAD DEL PROCESO DE GESTIÓN DE INCIDENCIAS DE SOFTWARE BASADA EN COBIT 2019

Con el propósito de complementar los resultados obtenidos mediante el cuestionario de percepción de los usuarios y la Matriz Documental de Incidencias de Software, se aplicó la Matriz de Evaluación de Capacidad del Proceso basada en COBIT 2019. Este instrumento permitió determinar el estado actual del proceso de gestión de incidencias de software en las áreas de Negocios y Operaciones de Banco Ficensa, establecer un nivel objetivo y precisar la brecha que deberá atenderse mediante la propuesta.

La evaluación se refiere exclusivamente a la gestión de las incidencias de software analizadas en la investigación. Por tanto, sus resultados no representan una valoración general de toda la Mesa de Servicio institucional ni de la totalidad de los procesos de TI del banco. Banco Ficensa ya dispone de una Mesa de Servicio para la gestión formal de distintas solicitudes tecnológicas. La brecha identificada se encuentra en que las incidencias relacionadas con el funcionamiento del software utilizado por las áreas de Negocios y Operaciones todavía no se incorporan de manera uniforme a dicho esquema.

Para realizar la valoración se tomó como base la información recopilada durante el año 2025. La Matriz Documental contiene 56 incidencias de software, de las cuales 35 fueron gestionadas mediante registros informales, equivalentes al 62.5%, mientras que 21 incidencias, equivalentes al 37.5%, cuentan con registros formales. Asimismo, 28 incidencias permanecían sin cierre documentado al finalizar el período analizado, representando el 50.0% del total. El tiempo promedio de atención inicial fue de 1.54 días y el tiempo promedio de resolución de las incidencias cerradas fue de 8.57 días. Estos resultados evidencian que existe una respuesta operativa ante las fallas reportadas, pero el proceso todavía no se ejecuta bajo un flujo único, obligatorio y completamente trazable.

4.2.3.1. RESULTADO DE LA EVALUACIÓN DE CAPACIDAD DEL PROCESO

La evaluación se realizó mediante los seis niveles de capacidad definidos en el instrumento: nivel 0, incompleto; nivel 1, ejecutado; nivel 2, gestionado; nivel 3, establecido; nivel 4, predecible; y nivel 5, optimizado. La Tabla 23 presenta la valoración del estado actual AS-IS y del estado objetivo TO-BE.

Tabla 24: Matriz de Evaluación de Capacidad del Proceso de Gestión de Incidencias de Software basada en COBIT 2019

Nivel	Nombre del nivel	Descripción COBIT	Criterios de evaluación del proceso	Estado AS-IS	Estado TO-BE	Brecha	Observaciones
0	Incompleto	El proceso no logra su propósito.	No existe una gestión de incidencias, no hay registros ni mecanismos de control.				Este nivel no representa la situación actual, debido a que las incidencias de software sí son atendidas por el área de TI. Aunque existen debilidades en la formalización, se cuenta con evidencia de atención de casos durante el período analizado.

Nivel	Nombre del nivel	Descripción COBIT	Criterios de evaluación del proceso	Estado AS-IS	Estado TO-BE	Brecha	Observaciones
1	Ejecutado	El proceso logra su propósito de forma básica.	Las incidencias son atendidas, pero no existe una documentación completa ni una estandarización uniforme.	X			Este nivel corresponde al estado actual del proceso. Las incidencias son comunicadas y atendidas; sin embargo, una parte significativa de los casos se gestiona mediante correos electrónicos, mensajería instantánea y coordinaciones directas. Esto limita la trazabilidad integral, dificulta el seguimiento y reduce la confiabilidad de la información histórica disponible.
2	Gestionado	El proceso es planificado y supervisado.	Existe control básico, seguimiento, responsables identificados y cierta organización del proceso.				El proceso no alcanza este nivel de forma consistente. Algunos casos cuentan con evidencia documental y seguimiento, pero no existe un registro obligatorio dentro de la Mesa de Servicio para todas las incidencias de software. Tampoco se aplican de manera uniforme criterios de clasificación, priorización, asignación, escalamiento y cierre.

Nivel	Nombre del nivel	Descripción COBIT	Criterios de evaluación del proceso	Estado AS-IS	Estado TO-BE	Brecha	Observaciones
3	Establecido	El proceso se encuentra definido y estandarizado.	Existen procedimientos documentados, roles definidos y un flujo estructurado para gestionar las incidencias.		X	2 niveles	Este nivel corresponde al estado objetivo inicial de la propuesta. Para alcanzarlo, las incidencias de software deberán incorporarse formalmente a la Mesa de Servicio existente mediante un flujo documentado que contemple registro, clasificación, priorización, asignación, escalamiento, seguimiento, resolución, validación del usuario y cierre formal.
4	Predecible	El proceso es medido y controlado.	Se utilizan indicadores, monitoreo del desempeño, acuerdos de nivel de servicio y mecanismos de control de tiempos.				Este nivel podrá plantearse como una etapa posterior. Requiere que el flujo formal propuesto se encuentre implementado y que genere datos confiables durante un período suficiente para medir tendencias, controlar desviaciones y evaluar el cumplimiento de los tiempos establecidos.

Nivel	Nombre del nivel	Descripción COBIT	Criterios de evaluación del proceso	Estado AS-IS	Estado TO-BE	Brecha	Observaciones
5	Optimizado	El proceso se mejora continuamente.	La mejora se fundamenta en métricas, análisis de tendencias, lecciones aprendidas e innovación del proceso.				Este nivel corresponde a una fase futura de madurez. Para alcanzarlo será necesario analizar causas recurrentes, revisar periódicamente los indicadores, promover acciones preventivas y establecer mecanismos de mejora continua basados en evidencia.

Fuente: Elaboración propia con base en los resultados del cuestionario de percepción, la Matriz Documental de Incidencias de Software y los criterios de capacidad del proceso establecidos en el instrumento basado en COBIT 2019.

4.2.3.2. ANÁLISIS DEL ESTADO ACTUAL AS-IS

El proceso actual se ubica en el nivel 1 de capacidad, denominado “Ejecutado”. Esta valoración significa que las incidencias de software son atendidas por el área de TI y que el proceso cumple su propósito de forma básica; sin embargo, su ejecución todavía depende en gran medida de mecanismos informales y de coordinaciones individuales. La existencia de atención operativa permite descartar el nivel 0, pero la ausencia de un flujo obligatorio y estandarizado impide considerar que el proceso se encuentra gestionado de forma consistente.

La alta proporción de registros informales constituye una de las principales evidencias de esta situación. De las 56 incidencias analizadas, 35 fueron gestionadas mediante registros informales, equivalentes al 62.5%. El área de Operaciones presenta la mayor dependencia de este tipo de medios, con 27 incidencias informales de un total de 36 casos, equivalentes al 75.0%. En el área de Negocios, 8 de las 20 incidencias fueron gestionadas informalmente, representando el 40.0%.

Esta forma de trabajo dificulta reconstruir el historial completo de cada caso. Cuando una incidencia se reporta mediante mensajería instantánea, correo electrónico o comunicación directa,

la atención puede realizarse, pero no necesariamente quedan documentados todos los elementos requeridos para asegurar su trazabilidad: fecha de reporte, prioridad, impacto operativo, responsable asignado, acciones realizadas, fecha de resolución, validación del usuario y evidencia de cierre.

Otro resultado que refuerza la valoración es que 28 de las 56 incidencias permanecían sin cierre documentado al finalizar el período analizado. Esto no significa necesariamente que todos los casos continuaban afectando la operación, ya que algunos pudieron haber sido atendidos sin registrar formalmente su resolución. Sin embargo, desde la perspectiva del control del proceso, la ausencia de evidencia impide confirmar si el servicio fue restaurado, si el usuario quedó conforme con la solución o si la falla requiere seguimiento adicional.

La variabilidad en los tiempos también muestra la necesidad de formalizar el proceso. Aunque el tiempo promedio de atención inicial fue de 1.54 días y la mitad de las incidencias fueron atendidas el mismo día de su reporte, se identificó un caso con un tiempo de primera atención de hasta 20 días. En cuanto a la resolución, el promedio de los casos cerrados fue de 8.57 días, con una mediana de 4.5 días y un valor máximo de 43 días. Estas diferencias reflejan que la atención no se rige todavía por tiempos máximos uniformes ni por reglas documentadas de escalamiento.

El nivel 1 no debe interpretarse como una ausencia total de gestión ni como una falta de capacidad técnica del personal. La evidencia muestra que existe atención de incidencias y que el área de TI responde ante las fallas reportadas. La debilidad principal se encuentra en la estructura del proceso: no todas las incidencias ingresan por el mismo canal, no siempre existe un registro verificable y el seguimiento depende parcialmente de la comunicación entre las personas involucradas.

4.2.3.3. ESTADO OBJETIVO TO-BE Y BRECHA IDENTIFICADA

El estado objetivo inicial se establece en el nivel 3 de capacidad, denominado “Establecido”. En este nivel, el proceso debe encontrarse formalmente documentado, con actividades claramente definidas, responsables identificados y un flujo estructurado que pueda aplicarse de manera uniforme.

La brecha entre el estado actual y el estado objetivo es de dos niveles de capacidad. Para cerrar esta diferencia no se requiere implementar una nueva Mesa de Servicio, debido a que Banco Ficensa ya cuenta con una herramienta institucional para gestionar solicitudes tecnológicas. La

propuesta debe concentrarse en incorporar las incidencias de software de Negocios y Operaciones a la estructura existente mediante un flujo formal basado en ITIL 4.

El flujo deberá contemplar como mínimo las siguientes etapas:

1. Registro formal de la incidencia en la Mesa de Servicio existente.
2. Validación de la información proporcionada por el usuario.
3. Clasificación según el sistema afectado y el tipo de falla.
4. Priorización mediante criterios de impacto y urgencia.
5. Asignación al responsable o grupo técnico correspondiente.
6. Escalamiento funcional o jerárquico cuando el caso lo requiera.
7. Seguimiento de las acciones realizadas y de los tiempos transcurridos.
8. Registro de la solución aplicada.
9. Validación de la restauración del servicio por parte del usuario.
10. Cierre formal de la incidencia con evidencia verificable.

La formalización de estas etapas permitirá que cada caso disponga de un historial completo y consultable. Además, facilitará el cálculo periódico de indicadores como el tiempo promedio de atención, el tiempo promedio de resolución, el porcentaje de incidencias resueltas dentro del tiempo establecido, la tasa de reincidencia, el porcentaje de incidencias sin cierre y la distribución de casos por sistema, criticidad y área afectada.

4.2.3.4. IMPLICACIONES OPERATIVAS DE LA BRECHA

La brecha identificada tiene implicaciones directas para la operación del banco. Cuando las incidencias de software no se registran bajo un mismo esquema, resulta difícil conocer el volumen real de fallas, determinar cuáles sistemas requieren mayor atención y establecer si los tiempos de respuesta son adecuados. Esto reduce la capacidad del área de TI para priorizar recursos y dificulta la toma de decisiones basada en datos confiables.

La falta de trazabilidad también representa un riesgo operativo. Una incidencia puede ser atendida de forma temporal sin que se identifique su causa recurrente, especialmente cuando el historial del caso queda distribuido entre diferentes canales de comunicación. Como resultado,

pueden repetirse fallas similares, aumentar los tiempos de interrupción y generarse afectaciones en procesos críticos de Negocios y Operaciones.

La incorporación de un flujo formal permitirá fortalecer el control sin reemplazar la Mesa de Servicio existente. La propuesta busca aprovechar la infraestructura institucional disponible y ampliar su alcance para incluir las incidencias de software que actualmente se gestionan de forma dispersa. De esta manera, el banco podrá avanzar desde una atención básica y parcialmente informal hacia un proceso documentado, uniforme y trazable.

4.2.3.5. SÍNTESIS DE LA EVALUACIÓN DE CAPACIDAD DE PROCESO

Tabla 25: Síntesis de la Evaluación de Capacidad del Proceso

Elemento evaluado	Resultado
Proceso evaluado	Gestión de incidencias de software en las áreas de Negocios y Operaciones
Alcance de la evaluación	Incidencias de software identificadas durante el año 2025
Total de incidencias analizadas	56
Registros informales	35 incidencias, equivalentes al 62.5%
Registros formales	21 incidencias, equivalentes al 37.5%
Incidencias sin cierre documentado	28 incidencias, equivalentes al 50.0%
Tiempo promedio de atención inicial	1.54 días
Tiempo promedio de resolución de los casos cerrados	8.57 días
Nivel actual AS-IS	Nivel 1: Ejecutado
Nivel objetivo inicial TO-BE	Nivel 3: Establecido
Brecha identificada	2 niveles de capacidad
Enfoque de la propuesta	Incorporar un flujo formal para la gestión de incidencias de software dentro de la Mesa de Servicio existente

Fuente: Elaboración propia con base en los resultados de la investigación.

La evaluación confirma que Banco Ficensa dispone de una base operativa sobre la cual puede fortalecerse la gestión de incidencias de software. El reto principal es incorporar las incidencias de software al esquema institucional existente mediante reglas claras, registros obligatorios, criterios de prioridad, responsables definidos y mecanismos verificables de seguimiento y cierre. El nivel 3 constituye un objetivo inicial alcanzable y coherente con el alcance de la propuesta. Posteriormente, una vez que el flujo formal se encuentre en funcionamiento y genere información histórica confiable, el banco podrá avanzar hacia niveles superiores de capacidad orientados al monitoreo del desempeño y a la mejora continua.

4.2.4. INDICADORES CLAVE DE DESEMPEÑO (KPIS)

A partir de la matriz documental consolidada de incidencias de software correspondiente al año 2025, se estableció una línea base de indicadores clave de desempeño para evaluar el estado actual del proceso de atención en las áreas de Negocios y Operaciones de Banco Ficensa. La línea base permite transformar los registros históricos en información cuantitativa útil para identificar brechas operativas, medir la oportunidad de la atención, evaluar la eficiencia de la resolución y determinar el nivel de reincidencia de las fallas.

El análisis se realizó sobre un total de 56 incidencias de software identificadas durante el período de estudio. De los seis indicadores definidos en el instrumento presentado en el Anexo 3, cuatro pueden calcularse con la información histórica disponible. Los dos indicadores restantes deberán medirse después de incorporar formalmente las incidencias de software dentro de la Mesa de Servicio institucional y aplicar el flujo propuesto.

4.2.4.1. RESULTADOS CONSOLIDADOS DE LA LÍNEA BASE

Tabla 26. Resultados consolidados de los indicadores clave de desempeño (KPIs).

#	Indicador	Fórmula aplicada	Cálculo	Resultado 2025
1	Porcentaje de incidencias gestionadas sin registro formal	$(\text{Incidencias sin registro formal} / \text{Total de incidencias}) \times 100$	$(35 / 56) \times 100$	62.50%
2	Tiempo promedio de atención	$\Sigma \text{tiempos de atención} / \text{Total de incidencias con datos verificables}$	$\Sigma \text{tiempos} / 56$	1.54 días
3	Tiempo promedio de resolución (MTTR)	$\Sigma \text{tiempos de resolución} / \text{Total de incidencias resueltas con datos completos}$	$\Sigma \text{tiempos} / 28$	8.57 días
4	Tasa de reincidencia	$(\text{Incidencias reincidentes} / \text{Total de incidencias}) \times 100$	$(24 / 56) \times 100$	42.86%
5	Cumplimiento de acuerdos de nivel de servicio (SLA)	$(\text{Incidencias gestionadas dentro del SLA} / \text{Total evaluadas}) \times 100$	No aplicable	Seguimiento futuro
6	Porcentaje de incidencias con trazabilidad completa	$(\text{Incidencias con trazabilidad completa} / \text{Total registradas}) \times 100$	No aplicable	Seguimiento futuro

Fuente: Elaboración propia con base en la Matriz Documental de Incidencias de Software del año 2025.

Los resultados consolidados evidencian la existencia de brechas operativas relevantes en el proceso actual de gestión de incidencias de software, particularmente en las dimensiones de formalización del registro, eficiencia en la resolución y control de la recurrencia de fallas.

4.2.4.2.PORCENTAJE DE INCIDENCIAS GESTIONADAS SIN REGISTRO FORMAL

Este indicador mide la proporción de incidencias atendidas mediante canales no formalizados respecto al total de casos identificados. Su fórmula corresponde a:

Porcentaje de incidencias sin registro formal = $(\text{Incidencias sin registro formal} / \text{Total de incidencias identificadas}) \times 100$

Durante el año 2025 se identificaron 35 incidencias gestionadas mediante canales clasificados como informales, principalmente mensajería instantánea, frente a 21 incidencias con registro formal. Sobre un total de 56 casos, la aplicación de la fórmula genera un resultado de 62.50%. Esto significa que aproximadamente seis de cada diez incidencias de software fueron atendidas sin un expediente formal que permitiera reconstruir de manera completa su ciclo de vida.

El resultado evidencia que el proceso actual depende mayoritariamente de mecanismos de comunicación que no garantizan una trazabilidad uniforme. Aunque estos canales pueden facilitar una respuesta inmediata en determinados casos, su utilización como medio principal de reporte dificulta documentar aspectos esenciales como la fecha real de recepción, la asignación del responsable, las actividades realizadas, la solución implementada y la confirmación del cierre.

Esta condición limita la construcción de una base histórica confiable, reduce la capacidad para identificar patrones y dificulta la medición objetiva del desempeño del área de Desarrollo. Desde el punto de vista operativo, la ausencia de registros completos también puede generar reportes duplicados, pérdida de seguimiento y dependencia del conocimiento individual de las personas que participaron en la atención.

El hallazgo coincide con lo expuesto por Quiñónez Ku (2018), quien identificó que la falta de procesos estructurados para la gestión de incidencias limita la elaboración de informes, dificulta el control de los casos reportados y afecta la calidad del servicio. Asimismo, Tang y Todo (2013) destacan la importancia de contar con una Mesa de Servicio que funcione como punto único de contacto para centralizar la recepción y el seguimiento de los incidentes.

4.2.4.3.TIEMPO PROMEDIO DE ATENCIÓN

El tiempo promedio de atención mide el período transcurrido entre el reporte inicial de una incidencia y el inicio documentado de su atención. Su fórmula corresponde a:

Tiempo promedio de atención = Suma de tiempos de atención / Total de incidencias

con fecha de reporte y fecha de atención verificables

A partir de las 56 incidencias analizadas, se obtuvo un tiempo promedio de atención de 1.54 días. El valor mínimo fue de 0 días, lo que indica que algunos casos comenzaron a atenderse el mismo día de su reporte. El valor máximo alcanzó 20 días. La desviación estándar fue de 2.95 días, lo que evidencia una variación relevante entre los tiempos de respuesta inicial registrados.

El resultado no debe interpretarse de forma aislada como aceptable o inaceptable, debido a que durante el período analizado no existían SLA específicos para las incidencias de software. Sin embargo, la diferencia entre el valor mínimo y el máximo permite identificar una falta de uniformidad en la respuesta inicial. Mientras algunos casos fueron atendidos de forma inmediata, otros permanecieron varios días sin evidencia de atención.

La información disponible no permite determinar una causa única para esta variabilidad. No obstante, el comportamiento observado podría estar asociado con la ausencia de criterios homogéneos de priorización, la utilización de diferentes canales de reporte, la disponibilidad del personal técnico o la asignación informal de los casos. Cuando el proceso no dispone de reglas predefinidas, la oportunidad de la atención puede depender de la urgencia percibida por quien recibe el reporte y no necesariamente del impacto real sobre el negocio.

Desde una perspectiva operativa, esta variabilidad genera un riesgo relevante para el banco. Una incidencia que afecta un proceso crítico puede permanecer sin atención inicial durante un período superior al esperado, provocando retrasos, reprocesos o la utilización temporal de mecanismos manuales. Además, la ausencia de tiempos objetivo dificulta evaluar si el área responsable responde de manera consistente ante incidencias con características similares.

En consecuencia, la línea base de 1.54 días no debe utilizarse únicamente como un promedio general. También debe servir como referencia para definir tiempos de atención diferenciados según criticidad y establecer mecanismos de escalamiento cuando una incidencia no reciba respuesta dentro del plazo esperado.

4.2.4.4. TIEMPO PROMEDIO DE RESOLUCIÓN DE INCIDENCIAS (MTTR)

El indicador MTTR (Mean Time to Resolution) representa el promedio del tiempo transcurrido entre el reporte inicial de una incidencia y su solución documentada. Su fórmula corresponde a:

MTTR = Suma de tiempos de resolución / Total de incidencias resueltas con datos completos

Es necesario precisar que el MTTR de 8.57 días constituye una estimación conservadora del desempeño real del proceso. Al calcularse exclusivamente sobre las incidencias cerradas, el indicador está sujeto a un sesgo de censura estadística ya que los casos de mayor duración tienden a permanecer sin resolver y, por tanto, quedan excluidos del cálculo. En consecuencia, el tiempo de resolución real del proceso es necesariamente igual o superior al valor reportado.

Para dimensionar esta limitación se analizó la antigüedad de las incidencias abiertas, medida desde su fecha de reporte hasta el cierre del período de estudio (31 de diciembre de 2025). De las 28 incidencias sin resolver, 16 contaban con fecha de reporte verificable, sobre este subconjunto, la antigüedad promedio ascendió a 193 días, con una mediana de 214.5 días y un rango de 40 a 341 días. Este valor equivale a más de veintidós veces el MTTR de los casos cerrados (8.57 días), lo que confirma que la carga pendiente agrava sustancialmente el desempeño real del proceso. Dado que estas incidencias permanecían abiertas, dicha antigüedad representa un valor mínimo del tiempo que tomaría su resolución definitiva.

Las 12 incidencias restantes no disponían de fecha de reporte verificable ni de evidencia de seguimiento posterior, situación que impidió calcular su antigüedad. Esta ausencia de registro no constituye únicamente una limitación de los datos, sino que evidencia por sí misma la debilidad de trazabilidad del proceso actual: son casos que fueron reportados pero que carecen de historial documentado desde su origen hasta su estado final. Este comportamiento refuerza la necesidad de un registro formal y un mecanismo de seguimiento obligatorio como los que incorpora el modelo propuesto.

El cálculo se realizó únicamente sobre las 28 incidencias que contaban con fecha de reporte y fecha de resolución verificables. El MTTR obtenido fue de 8.57 días. La mediana fue de 4.50 días, el valor mínimo fue de 0 días y el valor máximo alcanzó 43 días.

La diferencia entre la media de 8.57 días y la mediana de 4.50 días evidencia que algunos casos presentaron tiempos de resolución considerablemente superiores al comportamiento habitual. Esto implica que el promedio general se encuentra influido por incidencias que permanecieron abiertas durante períodos prolongados. Por tanto, el MTTR debe interpretarse conjuntamente con la distribución de los tiempos y no como una medida aislada.

Al igual que en el indicador anterior, no es posible afirmar si el resultado cumple o

incumple las expectativas del negocio, debido a que las incidencias de software no disponían de SLA específicos durante el período analizado. Sin embargo, el hallazgo permite identificar tres brechas relevantes:

- La ausencia de tiempos objetivo impide evaluar formalmente el cumplimiento del proceso.
- La existencia de casos con tiempos prolongados sugiere la necesidad de fortalecer el seguimiento y el escalamiento de incidencias que excedan determinados umbrales.
- El hecho de que la mitad de los casos analizados permanezca sin una resolución documentada limita la trazabilidad y dificulta determinar si el servicio fue restaurado de manera definitiva.

Este resultado guarda relación con lo señalado por Ayala Soto y Caso Rojas (2023), quienes sostienen que la adopción de buenas prácticas de ITIL 4 favorece el control de los tiempos de atención y resolución. Asimismo, la formalización del proceso permitiría establecer compromisos diferenciados según criticidad, supervisar los casos abiertos y generar alertas cuando una incidencia exceda el tiempo esperado.

4.2.4.5.TASA DE REINCIDENCIA

La tasa de reincidencia mide la proporción de incidencias que se repiten en el mismo sistema, módulo o proceso respecto al total de casos identificados. Su fórmula corresponde a:

$$\text{Tasa de reincidencia} = (\text{Incidencias reincidentes} / \text{Total de incidencias identificadas}) \times 100$$

De las 56 incidencias analizadas, 24 fueron clasificadas como reincidentes y 32 como no reincidentes. La aplicación de la fórmula genera una tasa de reincidencia de 42.86%. Esto significa que más de cuatro de cada diez casos identificados durante el año 2025 estuvieron asociados con fallas previamente observadas en el mismo sistema, módulo o proceso.

El resultado evidencia que una proporción relevante de las incidencias no corresponde a eventos aislados. La recurrencia puede estar asociada con soluciones temporales, causas subyacentes que no han sido eliminadas o dependencias tecnológicas que continúan generando afectaciones. El análisis documental no permite determinar por sí solo la causa raíz de cada caso; sin embargo, sí permite identificar sistemas que requieren una evaluación más profunda.

La distribución por sistema muestra que Inclusión Financiera concentra 12 incidencias

reincidentes, todas clasificadas como “Sin Resolver”. El sistema ENEE presenta siete incidencias reincidentes, todas registradas como resueltas. Asimismo, se identificaron recurrencias en RAP, Conciliación SINAP y Alcaldía Municipal del Distrito Central.

Estas diferencias permiten identificar situaciones que deben analizarse de forma separada. En el caso de Inclusión Financiera, la repetición de incidencias sin resolución documentada sugiere la existencia de una afectación persistente que requiere seguimiento específico. En el caso de ENEE, la reincidencia de casos registrados como resueltos podría indicar que la restauración del servicio no ha eliminado completamente la causa subyacente o que existen diferentes eventos asociados con una misma integración tecnológica.

Desde la perspectiva de ITIL 4, la Gestión de Incidencias tiene como propósito restaurar la operación normal del servicio en el menor tiempo posible. No obstante, cuando una falla se repite, resulta necesario articular la atención operativa con la práctica de Gestión de Problemas, orientada a identificar y tratar las causas reales o potenciales de los incidentes.

En el caso de Banco Ficensa, la tasa de reincidencia de 42.86% justifica la incorporación de mecanismos para identificar casos repetitivos, escalar su análisis y vincularlos con acciones de causa raíz cuando corresponda.

4.3. HALLAZGOS PRINCIPALES

4.3.1. ANÁLISIS DERIVADOS DE LOS RESULTADOS

A continuación, se presentan los hallazgos de la investigación de acuerdo con los seis objetivos específicos planteados. Para su elaboración se integraron los resultados del cuestionario de percepción aplicado a los usuarios, la Matriz Documental de Incidencias de Software correspondiente al año 2025, la Matriz de Evaluación de Capacidad del Proceso basada en COBIT 2019 y la matriz de indicadores clave de desempeño. Esta lectura conjunta permitió identificar no solo las cifras más relevantes, sino también las brechas operativas que deben atenderse mediante la propuesta.

Tabla 27: Hallazgos principales derivados del análisis de resultados

Objetivo específico	Hallazgo principal	Sustento de resultados
Objetivo 1. Analizar la situación actual de la gestión de incidencias de software en las áreas de Negocios y Operaciones durante 2025.	La gestión actual permite atender las fallas reportadas, pero todavía presenta debilidades en la formalización, la trazabilidad y el control operativo.	Durante el año 2025 se identificaron 56 incidencias de software que afectaron a 32 sistemas distintos. Los reportes se distribuyeron entre diferentes medios, principalmente Microsoft Teams, correo electrónico y comunicaciones directas. La evaluación de capacidad basada en COBIT 2019 ubicó el estado actual AS-IS en el nivel 1, denominado “Ejecutado”. Esto significa que las incidencias son atendidas, pero el proceso aún depende en buena medida de prácticas informales y no se aplica bajo un flujo uniforme para todos los casos.
Objetivo 2. Calcular el tiempo promedio de atención y resolución de las incidencias de software registradas durante 2025.	La atención inicial suele realizarse en un plazo relativamente corto, pero la resolución definitiva presenta diferencias importantes entre los casos.	El tiempo promedio de atención inicial fue de 1.54 días. En cuanto a la resolución, el promedio fue de 8.57 días para las 28 incidencias que contaban con cierre documentado. La mediana fue de 4.5 días y el tiempo máximo alcanzó 43 días. Además, las incidencias de criticidad alta registraron un promedio de resolución de 13.25 días. Estos resultados muestran que algunos casos se atienden con rapidez, mientras que otros permanecen abiertos durante períodos prolongados, sin que exista todavía un esquema uniforme de tiempos objetivo y reglas de escalamiento.
Objetivo 3. Clasificar y cuantificar las incidencias según tipo, criticidad y área afectada.	Las incidencias se concentran principalmente en el área de Operaciones, en fallas funcionales y en sistemas que requieren seguimiento específico por su recurrencia.	Operaciones concentró 36 de las 56 incidencias, equivalentes al 64.3% del total. El tipo de incidencia predominante fue la falla funcional, con 38 casos, equivalentes al 67.9%. La criticidad media también representó el 67.9% de los registros. El sistema Inclusión Financiera acumuló 12 incidencias, siendo el de mayor concentración y reincidencia. Esta distribución permite reconocer puntos de atención prioritaria y orientar los esfuerzos de mejora hacia los sistemas con mayor impacto operativo.
Objetivo 4. Determinar el porcentaje de incidencias gestionadas sin registro formal durante 2025.	La informalidad representa una de las principales brechas del proceso actual y afecta la confiabilidad de la información histórica.	De las 56 incidencias analizadas, 35 fueron gestionadas sin un registro formal, equivalentes al 62.5% del total. La situación es más marcada en Operaciones, donde 27 de 36 incidencias fueron informales, representando el 75.0%. En Negocios, 8 de 20 incidencias fueron gestionadas informalmente, equivalentes al 40.0%. Cuando un caso se atiende mediante mensajes, llamadas o coordinaciones directas, puede resolverse operativamente, pero no siempre queda evidencia completa de su apertura, responsable, seguimiento, solución y cierre.

Objetivo específico	Hallazgo principal	Sustento de resultados
Objetivo 5. Establecer indicadores de desempeño para evaluar la gestión de incidencias de software del área de Desarrollo.	La investigación permitió construir una línea base inicial de indicadores y definir las métricas que deberán monitorearse periódicamente cuando se formalice el proceso.	La matriz documental permitió calcular indicadores como el tiempo promedio de atención, el tiempo promedio de resolución, la tasa de resolución, el porcentaje de incidencias sin cierre documentado, la tasa de reincidencia y el porcentaje de registros informales. La tasa de reincidencia alcanzó el 42.86%, equivalente a 24 casos, mientras que el 50.0% de las incidencias no contaba con cierre documentado. A partir de estos resultados se definió una matriz de KPIs que incorpora tanto indicadores de línea base como métricas futuras de seguimiento, entre ellas el cumplimiento de SLA y la distribución de incidencias por sistema, área, tipo y criticidad.
Objetivo 6. Definir un flujo formal de registro, clasificación, escalamiento, seguimiento y cierre de incidencias de software.	Los resultados respaldan la incorporación de un flujo formal de incidencias de software dentro de la Mesa de Servicio existente, sin necesidad de implementar una nueva herramienta.	La evaluación de capacidad identificó una brecha de dos niveles entre el estado actual AS-IS, ubicado en el nivel 1 “Ejecutado”, y el estado objetivo TO-BE, establecido en el nivel 3 “Establecido”. Para cerrar esta brecha se requiere integrar las incidencias de software a la Mesa de Servicio institucional mediante un flujo documentado que incluya registro, validación, clasificación, priorización, asignación, escalamiento, seguimiento, resolución, validación del usuario y cierre formal. La aceptación de los usuarios favorece esta transición: el 83.64% considera que una gestión centralizada mejoraría el proceso y el 84.55% manifiesta disposición para utilizar con frecuencia un canal formal.

Fuente: Elaboración propia con base en el cuestionario de percepción de usuarios, la Matriz Documental de Incidencias de Software del año 2025, la Matriz de Evaluación de Capacidad del Proceso basada en COBIT 2019 y la matriz de indicadores clave de desempeño.

En conjunto, los resultados muestran que Banco Ficensa no parte de una ausencia total de gestión. Las incidencias de software son atendidas y existe una base operativa que puede aprovecharse. El problema se encuentra en que la atención todavía no se desarrolla bajo un procedimiento común, obligatorio y verificable para todos los casos.

La propuesta debe responder a esta brecha mediante la incorporación de un flujo formal dentro de la Mesa de Servicio institucional. Esto permitirá mejorar la trazabilidad, ordenar la asignación de responsables, definir tiempos esperados según la criticidad, establecer reglas de escalamiento y generar información confiable para evaluar el desempeño del proceso de forma periódica.

4.3.2. ANÁLISIS DE RIESGOS E IMPLICACIONES ESTRATÉGICAS DERIVADOS DE LOS HALLAZGOS

Los hallazgos principales de la investigación permiten evidenciar que las brechas actuales en la gestión de incidencias de software no solo representan limitaciones operativas, sino también riesgos relevantes para la continuidad del negocio bancario, el gobierno de TI y la toma de decisiones institucional. La existencia de incidencias gestionadas por canales informales, la falta de cierre documentado, los tiempos prolongados de resolución y la reincidencia de fallas reflejan debilidades que pueden afectar la trazabilidad, la productividad de las áreas usuarias y la capacidad del banco para controlar adecuadamente sus servicios tecnológicos.

Por esta razón, resulta necesario analizar los riesgos derivados de los principales hallazgos, considerando no solo el dato cuantitativo obtenido, sino también sus consecuencias prácticas para Banco Ficensa. En una institución financiera, las incidencias de software pueden impactar procesos críticos de Negocios y Operaciones, por lo que la ausencia de registros completos y de mecanismos formales de seguimiento puede limitar la capacidad de respuesta, dificultar auditorías internas y reducir la visibilidad gerencial sobre el desempeño del servicio.

Para la valoración de los riesgos identificados se adoptó un enfoque semicuantitativo alineado con la norma ISO 31000:2018, que estructura la gestión del riesgo en las etapas de identificación, análisis y evaluación (Organización Internacional de Normalización, 2018). Cada riesgo derivado de los hallazgos se analizó en función de dos criterios: la probabilidad de ocurrencia y el impacto potencial sobre la operación del banco. A partir del producto de ambos factores se determinó el nivel de riesgo, empleando una escala de cinco niveles que permite priorizar la atención de los riesgos conforme a su criticidad.

Tabla 28. Escala de valoración de la probabilidad.

Valor	Nivel	Descripción
1	Raro	Ocurrencia excepcional
2	Improbable	Podría ocurrir ocasionalmente
3	Posible	Ocurre en algunos casos
4	Probable	Ocurre con frecuencia
5	Casi seguro	Presente de forma sistemática

Fuente: Elaboración propia con base en ISO 31000:2028

Para el análisis de cada riesgo se definió una escala de probabilidad de cinco niveles, que expresa la frecuencia con la que el evento asociado podría materializarse dentro de la operación

del banco. Esta escala permite traducir la recurrencia observada en los hallazgos en un valor comparable entre riesgos.

Tabla 29. Escala de valoración del impacto.

Valor	Nivel	Descripción
1	Insignificante	Efecto mínimo, sin afectación operativa
2	Menor	Afectación leve y localizada
3	Moderado	Afectación operativa apreciable
4	Mayor	Afectación a procesos críticos o al control institucional
5	Catastrófico	Interrupción grave o incumplimiento regulatorio

Fuente: Elaboración propia con base en ISO 31000:2018

De manera complementaria, se estableció una escala de impacto de cinco niveles, orientada a valorar la magnitud de las consecuencias que cada riesgo tendría sobre la continuidad operativa, el control institucional y el gobierno de TI. En el contexto de una institución financiera, el impacto no se limita a la afectación técnica, sino que abarca la trazabilidad, la capacidad de auditoría y la confianza en el proceso de atención.

Tabla 30. Niveles de riesgo según la combinación de probabilidad e impacto.

Rango	Categoría
1 – 4	Bajo
5 – 9	Medio
10 – 15	Alto
16 – 25	Crítico

Fuente: Elaboración propia con base en ISO 31000:2018

A partir de la combinación de ambos factores, el nivel de riesgo se obtiene como el producto de la probabilidad por el impacto, lo que genera un valor entre 1 y 25. Este resultado se clasifica en cuatro categorías bajo, medio, alto y crítico que permiten priorizar la atención de los riesgos y orientar las medidas de tratamiento hacia aquellos de mayor criticidad.

Tabla 31: Riesgos e implicaciones estratégicas derivados de los hallazgos

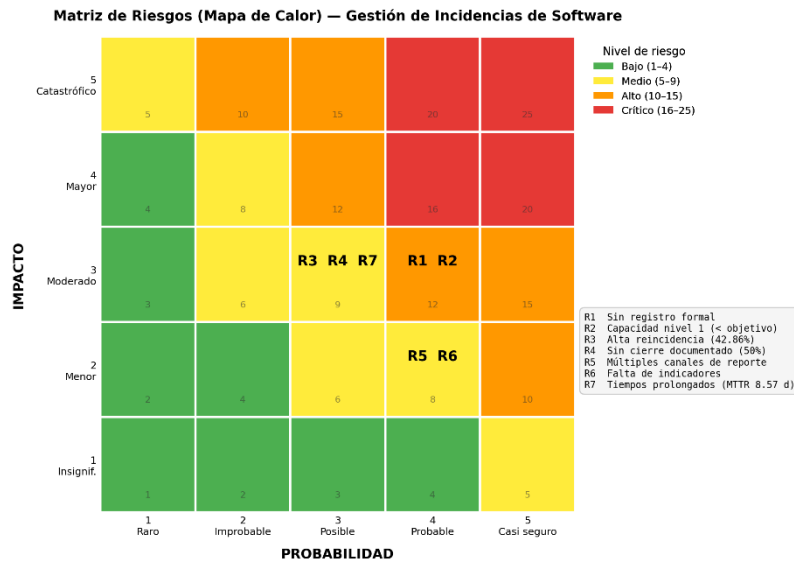
Hallazgo identificado	Riesgo derivado	Impacto organizacional	Implicación estratégica	P	I	Nivel	Categoría
Incidencias gestionadas sin registro formal	Falta de trazabilidad, pérdida de evidencia y dificultad para auditar	Dificultad para reconstruir el historial de los casos y verificar la atención brindada	Requiere formalizar el registro para fortalecer el control y la información institucional	4	3	12	Alto
Nivel de capacidad actual inferior	Proceso ejecutado pero no estandarizado bajo controles uniformes	Dependencia de prácticas informales y del conocimiento	Orienta la evolución hacia un proceso gestionado y sostenible	4	3	12	Alto

Hallazgo identificado	Riesgo derivado	Impacto organizacional	Implicación estratégica	P	I	Nivel	Categoría
al objetivo (nivel 1 vs. 3)		individual del personal	conforme a buenas prácticas				
Alta tasa de reincidencia	Persistencia de causas raíz no corregidas	Reprocesos y mayor carga de trabajo para los usuarios y el área de Desarrollo	Sugiere incorporar análisis de causas y mejora continua en el modelo	3	3	9	Medio
Incidentes sin cierre documentado	Dificultad para confirmar la restauración completa del servicio	Incertidumbre sobre si la falla fue efectivamente resuelta y validada por el usuario	Refuerza la necesidad de criterios formales de validación y cierre	3	3	9	Medio
Uso de múltiples canales de reporte	Dispersión de la información y dificultad para dar seguimiento	Confusión para los usuarios y menor eficiencia en la atención de incidencias	Respalda la centralización del proceso en una Mesa de Servicio	4	2	8	Medio
Falta de indicadores históricos consolidados	Dificultad para medir desempeño y priorizar recursos	Menor visibilidad gerencial sobre el comportamiento del proceso	Justifica la incorporación de un tablero de indicadores de seguimiento	4	2	8	Medio
Tiempos prolongados de resolución.	Retrasos en la recuperación de los servicios afectados	Prolongación de la afectación operativa en algunos casos	Orienta la definición de SLA y reglas de escalamiento por criticidad	3	3	9	Medio

Fuente: Elaboración propia con base en los resultados del cuestionario de percepción, la Matriz Documental de Incidencias de Software, la evaluación de capacidad basada en COBIT 2019 y la matriz de indicadores clave de desempeño.

La valoración evidencia que dos de los siete riesgos identificados alcanzan un nivel alto y los cinco restantes un nivel medio, sin que ninguno se ubique en el nivel crítico.

Figura 20. Matriz de riesgos (mapa de calor) de la gestión de incidencias de software.



Fuente: Elaboración propia con base en la valoración de riesgos conforme a ISO 31000:2018

En consecuencia, los hallazgos muestran que Banco Ficensa cuenta con una base operativa para atender incidencias, pero requiere avanzar hacia un modelo más formal, medible y alineado con buenas prácticas de gestión de servicios de TI. Esta transición permitiría mejorar el control institucional sobre los sistemas afectados, reducir reprocesos, prevenir fallas recurrentes y fortalecer la capacidad del banco para responder oportunamente ante eventos que puedan comprometer la operación de servicios críticos.

5. CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1.CONCLUSIONES

1. El diagnóstico comprobó que la gestión de incidencias de software en Banco FICENSA presenta una operación parcialmente informal y dispersa. El 62.5% de los casos analizados no contó con registro formal, el 50.0% permaneció sin cierre documentado y la evaluación basada en COBIT 2019 ubicó el proceso en el nivel 1 de capacidad, denominado “Ejecutado”. Estos hallazgos evidencian limitaciones en la trazabilidad, medición, seguimiento y control operativo de las incidencias. A partir de este diagnóstico, se diseñó un modelo basado en prácticas de Gestión de Incidencias de ITIL 4. Su implementación posterior podría mejorar la trazabilidad, formalizar las responsabilidades, facilitar la medición del desempeño y fortalecer el control operativo. Estos efectos constituyen beneficios esperados y no resultados comprobados, debido a que el modelo todavía no ha sido implementado ni evaluado en Banco FICENSA.
2. El análisis de la situación actual permitió comprobar que las incidencias de software en las áreas de Negocios y Operaciones sí reciben atención por parte del área de TI, pero su gestión todavía se realiza mediante prácticas que no siempre siguen un mismo criterio. Los reportes se distribuyen entre distintos medios y una parte importante de los casos no cuenta con un historial completo desde su apertura hasta su cierre. Esta situación limita la trazabilidad y dificulta conocer con precisión el comportamiento real del proceso. La evaluación basada en COBIT 2019 confirma esta condición al ubicar el estado actual en el nivel 1 de capacidad, denominado “Ejecutado”.
3. La medición de los tiempos mostró que existe una diferencia importante entre brindar una primera respuesta y alcanzar una resolución definitiva. El tiempo promedio de atención inicial fue de 1.54 días, mientras que el tiempo promedio de resolución alcanzó 8.57 días para los casos con cierre documentado. Aunque algunas incidencias fueron solucionadas rápidamente, otras permanecieron abiertas durante períodos prolongados, llegando hasta un máximo de 43 días. Esto demuestra la necesidad de establecer tiempos objetivo según el nivel de criticidad y reglas claras de escalamiento cuando una incidencia supera el plazo esperado.

4. La clasificación de las incidencias permitió identificar que el área de Operaciones concentra la mayor cantidad de casos, con 36 incidencias equivalentes al 64.3% del total. También se determinó que las fallas funcionales representan el tipo más frecuente, con 38 casos, y que Inclusión Financiera es el sistema con mayor concentración y reincidencia. Estos resultados permiten reconocer los puntos donde el banco debe enfocar inicialmente sus esfuerzos de seguimiento, sin descuidar el resto de los sistemas que soportan la operación diaria.
5. El porcentaje de incidencias gestionadas sin registro formal alcanzó el 62.5%, equivalente a 35 de los 56 casos analizados. Este resultado confirma que la informalidad no es una situación aislada, sino una característica relevante del proceso actual. Cuando una incidencia se atiende mediante mensajes, llamadas o coordinaciones directas, puede lograrse una solución operativa, pero se pierde parte de la evidencia necesaria para medir tiempos, identificar recurrencias, asignar responsabilidades y comprobar el cierre del caso.
6. La investigación permitió establecer una línea base de indicadores para evaluar la gestión de incidencias de software del área de Desarrollo. Entre los resultados más relevantes se encuentran el tiempo promedio de atención, el tiempo promedio de resolución, el porcentaje de registros informales, la tasa de reincidencia del 42.86% y el porcentaje de incidencias sin cierre documentado del 50.0%. Estos indicadores ofrecen un punto de partida para medir la evolución del proceso y deberán complementarse con métricas de cumplimiento de SLA una vez que el flujo formal se encuentre incorporado a la Mesa de Servicio.
7. La propuesta debe orientarse a integrar las incidencias de software dentro de la Mesa de Servicio que Banco Ficensa ya utiliza para otras solicitudes tecnológicas. No se requiere implementar una herramienta nueva, sino ampliar el alcance del esquema existente mediante un flujo formal basado en ITIL 4. La evaluación de capacidad estableció como objetivo inicial el nivel 3, denominado “Establecido”, lo que implica documentar las etapas de registro, validación, clasificación, priorización, asignación, escalamiento, seguimiento, resolución, validación del usuario y cierre formal. Este avance permitiría reducir la brecha actual de dos niveles y fortalecer el control operativo del proceso.
8. La concentración de 36 incidencias en Operaciones, equivalentes al 64.3% del total, puede

relacionarse con la dependencia de esta área respecto de aplicaciones transaccionales, procesos continuos e integraciones con entidades externas. Estas condiciones incrementan la exposición a errores de comunicación, procesamiento y funcionamiento. Además, el uso de canales informales y la documentación incompleta pueden ocasionar que incidencias similares se atiendan repetidamente sin conservar suficiente evidencia. Debido al alcance descriptivo del estudio, estas condiciones representan explicaciones plausibles y no relaciones causales comprobadas.

5.2. RECOMENDACIONES

1. Se recomienda implementar gradualmente el modelo de Gestión de Incidencias de Software dentro de ManageEngine ServiceDesk Plus, iniciando con una prueba piloto en las áreas de Negocios y Operaciones. La implementación deberá incluir responsables, campos obligatorios, criterios de clasificación y priorización, SLA, reglas de escalamiento, seguimiento documentado, validación del usuario y cierre formal. Posteriormente, los resultados deberán compararse con la línea base de 2025, considerando el porcentaje de registros formales, incidencias con cierre documentado, tiempos de atención y resolución, reincidencia y cumplimiento de SLA. Esta evaluación permitirá comprobar si el modelo mejora la trazabilidad, el control operativo y el desempeño del proceso, evitando presentar los beneficios esperados como resultados garantizados.
2. Incorporar todas las incidencias de software de las áreas de Negocios y Operaciones dentro de la Mesa de Servicio institucional, utilizando un procedimiento único de registro y seguimiento. Aunque una falla sea comunicada inicialmente por Teams, correo electrónico, llamada telefónica o de manera directa, deberá convertirse en un ticket formal. Esta medida permitirá conservar el historial de cada caso y reducir la dispersión de información que actualmente afecta la trazabilidad.
3. Definir tiempos objetivo de atención inicial y resolución según el nivel de criticidad de cada incidencia. Estos tiempos deberán acompañarse de alertas de vencimiento y reglas de escalamiento para los casos que permanezcan abiertos más allá del plazo establecido. La definición de estos criterios permitirá evitar que una incidencia relevante dependa únicamente del seguimiento manual de los usuarios o de la disponibilidad del personal

técnico.

4. Priorizar el seguimiento de los sistemas y áreas con mayor concentración de incidencias, especialmente el área de Operaciones, las fallas funcionales y el sistema Inclusión Financiera. Este monitoreo deberá incluir revisiones periódicas de recurrencia y, cuando corresponda, la vinculación con la práctica de Gestión de Problemas para identificar causas subyacentes. La prioridad no debe limitarse al volumen de casos, sino considerar también su impacto en la continuidad operativa.
5. Establecer como obligatorios los campos mínimos que debe contener cada ticket de incidencia de software: fecha y hora del reporte, área afectada, sistema involucrado, descripción de la falla, impacto, urgencia, prioridad asignada, responsable, acciones realizadas, solución aplicada, validación del usuario y fecha de cierre. Esto facilitará la reconstrucción del ciclo de vida de cada caso y mejorará la calidad de la información utilizada para auditoría, seguimiento y toma de decisiones.
6. Formalizar la matriz de indicadores clave de desempeño y revisarla de manera periódica. Como mínimo, deberán monitorearse el tiempo promedio de atención, el tiempo promedio de resolución, el cumplimiento de SLA, la tasa de resolución, el porcentaje de incidencias sin cierre documentado, la tasa de reincidencia, el porcentaje de registros informales y la distribución de incidencias por sistema, área, tipo y criticidad. La revisión de estos indicadores permitirá evaluar si el flujo formal realmente está generando mejoras y detectar oportunamente nuevas brechas.
7. Implementar gradualmente el flujo formal basado en ITIL 4 dentro de la Mesa de Servicio existente. La puesta en marcha deberá incluir una definición clara de roles y responsables, criterios de clasificación y priorización, reglas de escalamiento, seguimiento documentado, validación del usuario y cierre formal. También se recomienda acompañar el cambio con una comunicación breve a los usuarios y una orientación práctica sobre el canal que deberán utilizar. Una vez que el proceso se encuentre estabilizado y genere información confiable, el banco podrá avanzar hacia un nivel 4 de capacidad, orientado a la medición sistemática y al control del desempeño.
8. Se recomienda implementar un seguimiento específico de las incidencias de Operaciones, clasificándolas por sistema, tipo de falla, integración involucrada, criticidad, reincidencia

y canal de reporte. Mensualmente deberán identificarse los sistemas con mayor frecuencia de fallas funcionales, verificar el cumplimiento de los tiempos establecidos y documentar las acciones realizadas. Las incidencias repetitivas o de alto impacto deberán recibir prioridad y escalamiento dentro del flujo formal. Esto permitirá comprobar los patrones identificados, reducir la atención repetitiva y fortalecer el control operativo sin ampliar el alcance más allá de la Gestión de Incidencias de Software.

6. CAPÍTULO VI. APLICABILIDAD

6.1.NOMBRE DE LA PROPUESTA

MODELO INSTITUCIONAL PARA LA GESTIÓN DE INCIDENTES DE SOFTWARE BASADO EN ITIL 4 PARA BANCO FICENSA.

6.2.JUSTIFICACIÓN DE LA PROPUESTA

El modelo planteado responde directamente a las brechas identificadas en el análisis de la gestión de incidencias de software correspondiente al período 2025 en las áreas de Negocios y Operaciones de Banco FICENSA. Su diseño se sustenta en la evidencia recopilada mediante los instrumentos aplicados en la investigación, los cuales son:

- Cuestionario de percepción dirigido a los colaboradores.
- Matriz documental de incidencias.
- Matriz de evaluación de capacidad basada en COBIT 2019.

La convergencia de estos resultados delimitó con claridad las debilidades del proceso y fundamenta la pertinencia de una intervención estructurada. Los hallazgos que sustentan esta propuesta evidenciaron una dispersión de canales de reporte que coexisten sin una regla institucional compartida, lo que fragmenta la trazabilidad y limita la conservación de evidencia confiable; una proporción significativa de casos gestionados sin registro formal, particularmente en el área de Operaciones; una distancia considerable entre la primera respuesta brindada al usuario y la resolución definitiva del caso, reflejo de la ausencia de criterios formales de criticidad y reglas de escalamiento; y una recurrencia relevante de fallas en sistemas críticos, que confirma la necesidad de articular la atención operativa con la práctica de Gestión de Problemas

Finalmente, la evaluación de capacidad ubicó el proceso actual en el nivel Ejecutado, correspondiente al primer nivel de la escala de capacidad de COBIT 2019, con una brecha de dos niveles respecto al estado objetivo Establecido, lo que validó la necesidad de avanzar hacia un modelo formal, documentado y verificable.

El diseño planteado se sustenta en las bases conceptuales desarrolladas en el marco teórico. ITIL 4 constituye el eje principal del modelo, al aportar la lógica del Sistema de Valor del Servicio, la cadena de valor, las cuatro dimensiones de la gestión de servicios y la práctica

específica de Gestión de Incidencias, orientada a restaurar la operación normal del servicio en el menor tiempo posible (AXELOS, 2019). COBIT 2019 proporciona el componente de gobierno mediante el objetivo de gestión DSS02 "Gestionar las peticiones y los incidentes del servicio", cuyo modelo de capacidad otorga una referencia medible de progreso (ISACA, 2018). La integración de estas referencias permite que la solución no se limite a una mejora técnica, sino que adopte una perspectiva de gobernanza alineada con las exigencias del sector financiero hondureño.

La viabilidad de la intervención se sustenta en tres condiciones favorables identificadas durante la investigación:

- Banco FICENSA cuenta con una plataforma tecnológica adecuada que ya forma parte de su esquema institucional, por lo que la implementación no requiere la adquisición de una nueva herramienta, sino la ampliación funcional de la existente.
- Los usuarios manifestaron disposición favorable hacia la centralización del proceso y reconocieron la utilidad de un canal único, lo que reduce la resistencia esperada al cambio.
- El modelo se apoya en buenas prácticas internacionales ampliamente reconocidas, lo que le otorga consistencia metodológica y respaldo conceptual para su implementación en el contexto bancario nacional.

Las metas se proyectan a un horizonte inicial de doce meses posteriores a la puesta en operación y son consistentes con los límites aceptables formalizados en el componente 6.5 del presente capítulo, garantizando trazabilidad metodológica entre diagnóstico, propuesta y mecanismos de control.

Tabla 32. Beneficios cuantificables esperados de la implementación del modelo.

Indicador	Línea base 2025	Meta esperada con la propuesta	Fundamento técnico
Porcentaje de incidencias gestionadas sin registro formal	62.50%	Reducir a $\leq 15\%$ en seis meses y a $\leq 5\%$ en doce meses	Obligatoriedad del canal único en ServiceDesk Plus y registro asistido bajo excepción documentada.
Tiempo promedio de resolución (MTTR)	8.57 días	Reducir al menos 30% en los primeros seis meses, equivalente a un MTTR máximo esperado de 6.00 días	SLA diferenciados por criticidad, escalamiento automatizado y cierre formal del 100 % de los casos abiertos

Indicador	Línea base 2025	Meta esperada con la propuesta	Fundamento técnico
Tasa de reincidencia	42.86%	Reducir a $\leq 30\%$ en seis meses y a $\leq 20\%$ en doce meses	Análisis de causa raíz documentado en la Etapa 6, articulación con Gestión de Problemas y trazabilidad histórica consultable.
Incremento del nivel de capacidad COBIT	Nivel 1: Ejecutado	Alcanzar Nivel 3: Establecido	Procedimiento documentado, matriz RA de roles, flujo estandarizado de siete etapas y tablero institucional de indicadores
Cumplimiento de SLA (seguimiento futuro)	No medible para incidencias de software, debido a la ausencia de SLA específicos para este tipo de casos.	Un cumplimiento $\geq 85\%$	Tiempos objetivo formalizados por nivel de criticidad y supervisión automatizada en la plataforma
Trazabilidad completa del ciclo (seguimiento futuro)	No medible de forma confiable por ausencia de registro centralizado del ciclo completo.	Trazabilidad $\geq 90\%$	Registro obligatorio en las siete etapas y auditoría interna sobre ServiceDesk Plus

Fuente: Elaboración propia.

6.3.ALCANCE DE LA PROPUESTA

El alcance del presente modelo formal de gestión de incidencias de software para Banco FICENSA comprende el diseño integral de los componentes conceptuales, normativos y operativos que permitirán a la institución gestionar las incidencias de software de las áreas de Negocios y Operaciones bajo un esquema estructurado, alineado con las mejores prácticas definidas por ITIL 4 y con los objetivos de gobierno establecidos en COBIT 2019.

Esta intervención abarca la formulación de la política institucional que establecerá a ManageEngine ServiceDesk Plus como el único medio oficial de gestión de incidencias, así como el diseño del flujo de proceso de siete etapas que estandarizará las actividades de registro, validación, clasificación, priorización, asignación, diagnóstico y resolución, y validación y cierre de cada caso.

Asimismo, contempla la construcción de la matriz de criticidad, los acuerdos de nivel de servicio y las reglas de escalamiento, mediante las cuales se establecerán tiempos objetivo-diferenciados según el impacto operativo de la incidencia y la importancia estratégica del sistema afectado, garantizando que la respuesta institucional guarde proporción con la naturaleza del caso reportado.

El modelo incluye además la estructuración del esquema RA de roles y responsabilidades, orientado a delimitar con precisión las funciones del usuario reportante, la Mesa de Servicio, el área de Desarrollo, los líderes de proceso y la Gerencia de TIC dentro del ciclo completo de la incidencia, eliminando las ambigüedades operativas identificadas durante el diagnóstico.

De manera complementaria, integra el diseño del tablero de indicadores clave de desempeño, conformado por los seis KPIs definidos durante la investigación, que servirá como referencia metodológica para que la gerencia monitoree de forma periódica la trazabilidad, los tiempos de atención y resolución, la formalización del registro, la reincidencia, el cumplimiento de los acuerdos de servicio y la integridad del cierre documental.

Con el propósito de reducir ambigüedades en la interpretación del modelo propuesto, se delimita explícitamente el alcance de la propuesta a partir de sus principales dimensiones funcionales, tecnológicas y metodológicas. Esta delimitación permite precisar qué elementos forman parte del modelo y cuáles quedan fuera de su cobertura, manteniendo coherencia con los hallazgos del Capítulo IV, las recomendaciones del Capítulo V y los componentes desarrollados en el Capítulo VI.

Tabla 33. Matriz de delimitación del alcance de la propuesta.

Dimensión del alcance	Incluye	No incluye
Tipo de eventos	Incidencias de software reportadas por las áreas de Negocios y Operaciones, entendidas como interrupciones no planificadas o reducción en la calidad de un servicio, conforme a ITIL 4.	Incidentes de infraestructura, hardware, redes, telecomunicaciones, seguridad física o soporte técnico general al usuario.
Sistemas cubiertos	Sistemas críticos de negocio identificados en el diagnóstico documental del Capítulo IV, especialmente aquellos con mayor concentración de incidencias y reincidencias.	Componentes tecnológicos cuya afectación corresponda exclusivamente a infraestructura, redes, hardware o servicios fuera del ámbito de software.
Herramienta de registro y seguimiento	Integración funcional con ManageEngine ServiceDesk Plus como canal institucional para registrar, clasificar, priorizar, escalar, dar seguimiento y cerrar incidencias de software.	Adquisición de una nueva herramienta ITSM, sustitución de la Mesa de Servicio institucional o desarrollo de una plataforma adicional.
Gestión de niveles de servicio	Definición y seguimiento de SLA específicos para incidencias de software, diferenciados según criticidad, impacto operativo y urgencia técnica.	Gestión integral de niveles de servicio para todo el portafolio de servicios de TI del banco.
Flujo operativo	Registro, validación, clasificación, priorización, asignación, diagnóstico y resolución, validación del usuario y cierre formal.	Gestión de cambios, gestión de problemas y solicitudes de servicio generales como procesos formales independientes.
Reincidencia	Identificación y medición de reincidencias como indicador de control del modelo y como	Diseño completo de la práctica de Problem Management, análisis institucional de causa

Dimensión del alcance	Incluye	No incluye
	insumo para mejora continua.	raíz, administración de errores conocidos o eliminación estructural de fallas recurrentes.
Implementación proyectada	Cronograma, presupuesto, configuración sugerida, prueba piloto y puesta en marcha como ruta metodológica propuesta para una eventual adopción institucional.	Ejecución real de la implementación, aprobación formal del banco, parametrización definitiva en ambiente productivo, capacitación efectiva del personal y despliegue institucional completo.

Fuente: Elaboración propia.

A partir de esta delimitación, la propuesta queda circunscrita al diseño de un modelo formal, trazable y medible para la gestión de incidencias de software en Banco FICENSA. Los componentes relacionados con cronograma, presupuesto, configuración sugerida, prueba piloto y puesta en marcha se presentan como una ruta metodológica proyectada, sin implicar que dichas actividades hayan sido ejecutadas durante la investigación

6.3.1. OBJETIVO GENERAL

Diseñar un modelo formal de gestión de incidencias de software basado en ITIL 4 para las áreas de Negocios y Operaciones de Banco FICENSA, integrado conceptualmente a la plataforma ManageEngine ServiceDesk Plus, que articule una política institucional, un flujo de proceso estandarizado, una matriz de criticidad, una distribución formal de roles y un esquema de indicadores de desempeño, con el propósito de mejorar la trazabilidad, fortalecer el control operativo y elevar la capacidad del proceso conforme al estado objetivo identificado en la evaluación COBIT 2019.

6.3.2. OBJETIVOS ESPECÍFICOS

- Diseñar la política institucional de gestión de incidencias de software, que establezca el carácter obligatorio del registro formal de toda incidencia en la plataforma ManageEngine ServiceDesk Plus, independientemente del canal por el cual se reporte inicialmente.
- Definir el flujo formal de siete etapas del proceso de gestión de incidencias, que documente las actividades de registro, validación, clasificación, priorización, asignación, diagnóstico y resolución, y validación y cierre.
- Construir la matriz de criticidad, acuerdos de nivel de servicio y reglas de

escalamiento, que establezca tiempos objetivo de atención y resolución diferenciados según el impacto operativo del caso y los sistemas afectados.

- Establecer el modelo RA de roles y responsabilidades, que delimite las funciones del usuario reportante, la Mesa de Servicio, el área de Desarrollo, los líderes de proceso y la Gerencia de TIC dentro del ciclo completo de la incidencia.
- Estructurar el tablero de indicadores clave de desempeño, que integre los seis KPIs definidos durante la investigación como referencia para el monitoreo periódico del proceso por parte de la gerencia.

6.4.DESCRIPCIÓN Y DESARROLLO DE LA PROPUESTA

La presente sección desarrolla los cinco componentes que conforman el modelo formal de gestión de incidencias de software para las áreas de Negocios y Operaciones de Banco FICENSA. Cada componente responde a un objetivo específico de la propuesta y, en su conjunto, articula una solución integral que conecta la dimensión normativa, la dimensión operativa, la dimensión de gobierno y la dimensión de control del proceso.

Los cinco componentes desarrollados a continuación son: la política institucional de gestión de incidencias, el flujo formal de siete etapas, la matriz de criticidad y los acuerdos de nivel de servicio, el modelo RA de roles y responsabilidades, y el tablero de indicadores clave de desempeño. Su orden de presentación responde a una lógica de mayor a menor abstracción, partiendo del documento normativo institucional hasta llegar al instrumento de medición operativa.

6.4.1. POLÍTICA INSTITUCIONAL DE GESTIÓN DE INCIDENCIAS DE SOFTWARE

La formulación de una política institucional constituye el primer componente del modelo y representa el instrumento normativo que oficializa, dentro de Banco FICENSA, las reglas de actuación frente a las incidencias de software reportadas por las áreas de Negocios y Operaciones. Su diseño respondió de manera directa a los hallazgos del Capítulo IV, los cuales evidenciaron una dispersión de canales de reporte que coexistían sin una regla institucional compartida y una proporción significativa de casos gestionados al margen del registro formal.

La ausencia de un marco normativo unificado fue identificada durante el diagnóstico como una de las causas estructurales de la baja trazabilidad del proceso. En la práctica, cada

colaborador reportaba las incidencias según su criterio o costumbre, utilizando el correo electrónico, la plataforma Microsoft Teams, las llamadas telefónicas o la comunicación presencial.

Frente a este escenario, la política propuesta establece un marco normativo único que oficializa el carácter obligatorio del registro formal de toda incidencia de software en la plataforma ManageEngine ServiceDesk Plus, independientemente del canal por el cual se reporte inicialmente. Con ello, el banco no elimina los canales de comunicación existentes, sino que los subordina a un punto único de registro y trazabilidad institucional.

El diseño de la política se sustenta en el principio establecido por ITIL 4, según el cual toda incidencia debe ser registrada, clasificada y gestionada bajo un esquema uniforme con el fin de restaurar la operación normal del servicio en el menor tiempo posible (AXELOS, 2019). De igual manera, se alinea con el objetivo de gestión DSS02 de COBIT 2019, que exige la formalización del proceso de gestión de incidencias como condición para alcanzar niveles superiores de capacidad institucional (ISACA, 2018). Adicionalmente, la política guarda correspondencia con los requerimientos regulatorios y con el objetivo estratégico OE3 del Plan Estratégico de Tecnologías de Información y Comunicaciones de Banco FICENSA.

El diseño de la política incorpora además el marco de gobierno que exige el sector financiero hondureño. La Resolución No. 025-2022 de la Comisión Nacional de Bancos y Seguros establece la obligación de contar con una estructura formal de gobierno de tecnologías de información, con supervisión estratégica del Consejo de Administración y vigilancia de Auditoría Interna. En atención a este marco, la política asigna funciones diferenciadas al Comité de Riesgos Tecnológicos (o instancia equivalente), a la Gerencia de Tecnología y Comunicaciones y a la Unidad de Auditoría Interna.

A continuación, se presenta una síntesis estructurada de los elementos centrales de la política, los cuales fueron desarrollados conforme al formato institucional vigente para documentos normativos de Banco FICENSA.

6.4.1.1.SÍNTESIS ESTRUCTURADA DE LA POLÍTICA PROPUESTA

Tabla 34. Ficha de identificación documental de la política propuesta.

Código:	BF-GTI-POL.PYD.001-1.0.0
Clasificación:	Interno
Gerencia:	Gerencia de Tecnología y Comunicaciones
Fecha de emisión:	__/__/__
Elaborado por:	Ronaldo Enrrique Cárcamo Vásquez y Alex Gerardo Gámez Arteaga
Revisado por:	Jefe de Proyectos y Desarrollo
Aprobado por:	Gerente de Tecnología y Comunicaciones

Fuente: Se toma como base el formato oficial de políticas de Banco Ficensa.

Objetivo. Establecer las reglas institucionales que rigen el reporte, registro, atención, resolución y cierre formal de las incidencias de software que afectan la operación de las áreas de Negocios y Operaciones de Banco FICENSA, con el propósito de garantizar la trazabilidad completa del ciclo de vida de cada caso, asegurar tiempos de respuesta proporcionales al impacto operativo y fortalecer la capacidad institucional para prevenir su recurrencia.

Alcance. La política aplica a todos los colaboradores de las áreas de Negocios y Operaciones de Banco FICENSA y a todas las incidencias de software que afecten los sistemas utilizados para la operación bancaria. Quedan excluidas las incidencias de hardware, infraestructura de redes, telecomunicaciones y seguridad física, las cuales son atendidas por el área de Infraestructura, Redes y Comunicaciones bajo instrumentos normativos específicos, además de las incidencias de software relacionadas al core bancario, ya que tienen su propio canal de atención.

Definiciones. El documento incorpora un cuerpo de definiciones organizadas en orden alfabético, que comprende los términos canal único de gestión, ciclo de vida de la incidencia, escalamiento, incidencia, ManageEngine ServiceDesk Plus, Mesa de Servicio, registro formal y trazabilidad. Cada término se delimita con precisión para evitar ambigüedades interpretativas en su aplicación cotidiana.

Lineamientos generales. Toda incidencia de software que afecte la operación de las áreas de Negocios y Operaciones debe registrarse formalmente en la plataforma ManageEngine

ServiceDesk Plus dentro del tiempo definido por los acuerdos de nivel de servicio. Ningún caso debe atenderse, resolverse ni cerrarse fuera de la plataforma, aun cuando el reporte inicial se haya efectuado por un canal no institucional. El Oficial de Soporte Proyectos / Help Desk es responsable de garantizar la creación del registro institucional ante cualquier comunicación recibida por canales no oficiales, asegurando la documentación uniforme de la totalidad de los casos.

Roles y responsabilidades. La Gerencia de Tecnología y Comunicaciones es la autoridad responsable de la aprobación, vigencia y actualización del documento. El Jefe de Proyectos y Desarrollo coordina tácticamente la operación del modelo. El Oficial de Soporte Proyectos / Help Desk ejerce la función de Mesa de Servicio como primer nivel de atención, mientras que el Oficial de Soporte Cash Management cumple la misma función para los casos específicos de ese sistema. El Analista Programador Senior y los Analistas Programador Junior conforman el segundo nivel técnico responsable del diagnóstico, la resolución y la documentación técnica de los casos escalados, en tanto que las jefaturas de Negocios y Operaciones promueven la adopción de la política entre sus equipos y validan las soluciones brindadas antes del cierre formal.

Gobierno y supervisión. La política se inscribe en el sistema de gobierno corporativo de tecnologías de información de Banco FICENSA. La supervisión estratégica corresponde al Comité de Riesgos Tecnológicos o instancia equivalente designada por el Consejo de Administración, quien recibe los reportes consolidados de cumplimiento, autoriza las modificaciones de fondo y activa las acciones correctivas estructurales. La administración operativa corresponde a la Gerencia de Tecnología y Comunicaciones. La vigilancia independiente corresponde a la Unidad de Auditoría Interna, encargada de verificar el cumplimiento mediante revisiones semestrales documentales.

Disposiciones finales. El cumplimiento de la política será verificado semestralmente por la Unidad de Auditoría Interna sobre una muestra representativa de incidencias registradas en ManageEngine ServiceDesk Plus, evaluando cinco criterios obligatorios: existencia del registro formal, trazabilidad completa de las siete etapas, cumplimiento de los acuerdos de nivel de servicio, cierre formal validado por el usuario y consistencia entre criticidad y prioridad ejecutada.

La política se revisa de forma ordinaria con periodicidad anual y de forma extraordinaria ante cambios regulatorios, organizacionales o tecnológicos. El mecanismo de actualización contempla la elaboración de la propuesta por la Gerencia de TIC, validación del Comité de Riesgos

Tecnológicos cuando la modificación sea de fondo, aprobación formal y registro en el control de cambios.

Tabla 35. Elementos de gobernanza, revisión y cumplimiento de la política.

Elemento	Definición propuesta
Responsable formal de aprobación	Junta Directiva o Gerencia de Tecnología y Comunicaciones, según el nivel normativo que Banco FICENSA determine para la aprobación de la política.
Instancia de revisión previa	Comité de Tecnologías de Información, Comunicaciones y Seguridad de la Información, o la instancia de Gobierno de TI que Banco FICENSA designe formalmente.
Periodicidad de revisión	Revisión ordinaria anual y revisión extraordinaria ante cambios regulatorios, tecnológicos, organizacionales o hallazgos relevantes de auditoría.
Mecanismo de actualización	Control de versiones, control de revisiones, justificación del cambio, responsable de elaboración, responsable de revisión y responsable de aprobación, registrados en el control de cambios del documento normativo.
Criterios de auditoría y cumplimiento	Existencia del ticket, trazabilidad de las siete etapas, clasificación, criticidad, cumplimiento de SLA, escalamiento documentado, solución registrada y cierre validado por el usuario.
Vinculación con gobierno de TI y riesgo tecnológico	Reporte periódico a la Gerencia de Tecnología y Comunicaciones y al Comité de Tecnologías de Información, Comunicaciones y Seguridad de la Información; participación de Riesgos, Continuidad del Negocio, Riesgo Tecnológico y Auditoría Interna cuando aplique.

Fuente: Elaboración Propia

El documento completo en formato institucional, con sus elementos administrativos de control (codificación, marco legal tabulado, control de aprobación, control de cambios y anexos correspondientes), se presenta en el [Anexo 8](#) del presente Trabajo Final de Graduación.

6.4.2. FLUJO FORMAL DE SIETE ETAPAS DEL PROCESO DE GESTIÓN DE INCIDENCIAS

El segundo componente del modelo corresponde al diseño del flujo formal de siete etapas que estandariza la secuencia operativa por la cual debe atravesar toda incidencia de software desde su reporte inicial hasta su cierre documentado. Su desarrollo respondió de manera directa a uno de los hallazgos centrales del Capítulo IV, según el cual el proceso actual carecía de una secuencia uniforme de actuación, lo que generaba distancias considerables entre la primera respuesta brindada al usuario y la resolución definitiva del caso.

El diseño del flujo se sustenta en la cadena de valor del servicio definida por ITIL 4, la cual organiza las actividades de gestión en seis componentes interconectados: planificar, mejorar, involucrar, diseñar y transicionar, obtener y construir, y entregar y soportar (AXELOS, 2019). Dentro de esta cadena, la práctica específica de Gestión de Incidencias se materializa mediante

una secuencia de actividades que el modelo propuesto traduce en siete etapas concretas, adaptadas a la realidad operativa de Banco FICENSA y a las capacidades funcionales de la plataforma ManageEngine ServiceDesk Plus.

Las siete etapas que conforman el flujo son: registro, validación, clasificación, priorización, asignación, diagnóstico y resolución, y validación y cierre. Esta secuencia fue diseñada con un doble propósito. Por un lado, asegurar que toda incidencia atravesase de manera obligatoria por los puntos de control que el modelo COBIT 2019 exige para alcanzar el nivel objetivo de capacidad institucional (ISACA, 2018). Por otro lado, distribuir las responsabilidades técnicas y de validación entre los actores definidos en la política, evitando que un solo rol concentre la totalidad del ciclo y eliminando las ambigüedades operativas identificadas durante el diagnóstico.

6.4.2.1.ETAPA 1 - REGISTRO

Propósito. Garantizar que toda incidencia de software detectada por un colaborador de las áreas de Negocios u Operaciones quede registrada de forma directa y oportuna como un caso institucional dentro de ManageEngine ServiceDesk Plus, único medio oficial de gestión definido por el modelo. El registro constituye el punto de partida del ciclo de vida de la incidencia y, bajo el principio de autoservicio promovido por ITIL 4, es responsabilidad primaria del colaborador que detecta la falla.

Evento disparador. Detección de una incidencia de software por parte de un colaborador de las áreas de Negocios u Operaciones durante el desarrollo de su operación cotidiana, asociada a un sistema o módulo específico que presenta una interrupción no planificada o una degradación de la calidad del servicio.

Actor responsable (R). Colaborador reportante, quien efectúa el registro directamente en el portal de autoservicio de ManageEngine ServiceDesk Plus. De manera subsidiaria, el Oficial de Soporte Proyectos / Help Desk o el Oficial de Soporte Cash Management según el sistema afectado, únicamente bajo imposibilidad técnica documentada del colaborador, tal como la inoperatividad de su equipo, fallas de conectividad de red, problemas de credenciales de acceso o caídas de la propia plataforma.

Actor aprobador (A). Jefe de Proyectos y Desarrollo, en su rol institucional de coordinador táctico del modelo y responsable del desempeño general de la etapa, evaluable

mediante los indicadores definidos en el componente 6.5. La etapa no contempla aprobación caso a caso por cada ticket, conforme al principio de autoservicio promovido por ITIL 4.

Actividades específicas:

- Detectar la incidencia durante la operación del sistema afectado y documentar las condiciones en que se presentó.
- Acceder al portal de autoservicio de ManageEngine ServiceDesk Plus con las credenciales institucionales.
- Seleccionar la plantilla de ticket correspondiente al sistema o módulo afectado.
- Completar la totalidad de los campos obligatorios definidos por el modelo institucional.
- Adjuntar la evidencia disponible (capturas de pantalla, mensajes de error, descripción del comportamiento observado).
- Confirmar la creación del ticket y conservar el identificador único asignado para fines de seguimiento.

En los casos excepcionales de registro asistido, el colaborador comunica al Oficial de Soporte la imposibilidad técnica que le impide acceder al portal, el Oficial registra esta condición como justificación dentro del ticket, crea el ticket en nombre del colaborador con la información proporcionada, y una vez restablecido el acceso del colaborador, le notifica el identificador único del ticket para que la titularidad operativa retorne al reportante.

Entrada. Incidencia detectada por el colaborador durante su operación cotidiana, asociada a un sistema o módulo específico del banco.

Salida. Ticket institucional creado en ManageEngine ServiceDesk Plus con identificador único, fecha y hora exacta de registro, datos del reportante, descripción inicial de la incidencia y estado "Registrado", que habilita el inicio formal del ciclo de vida del caso.

Tabla 36. Tiempos, responsables y puntos de control etapa 1.

Tiempo máximo esperado	Responsable operativo	Responsable de aprobación/control	Punto de control automático propuesto en ServiceDesk Plus
10 minutos hábiles (uniforme para todos los niveles)	Colaborador reportante por autoservicio. Oficial de Soporte HD.	No aplica aprobación individual. El Jefe de Proyectos y Desarrollo	Preventivos: Validación de completitud de campos obligatorios;

	Oficial CM bajo registro asistido excepcional.	ejerce supervisión del desempeño general mediante los indicadores	bloqueo de envío sin evidencia adjunta cuando aplique. De trazabilidad: Generación automática del identificador único del ticket; sello automático de fecha y hora de registro; estado inicial "Registrado". Detectivos: Notificación automática al Oficial de Soporte al cierre del registro.
--	--	---	--

Fuente: Elaboración propia.

Campos del ticket creados en esta etapa (ManageEngine ServiceDesk Plus):

- Identificador único del ticket (generado automáticamente por la plataforma).
- Fecha y hora de registro.
- Nombre del reportante, área y unidad organizacional.
- Medio de contacto del reportante.
- Sistema o aplicación afectada declarada por el reportante.
- Módulo o funcionalidad específica declarada por el reportante.
- Descripción narrativa de la incidencia.
- Evidencia adjunta (*cuando aplique*).
- Modalidad de registro: Directo por el colaborador o Asistido por el Oficial.
- Justificación del registro asistido (*cuando aplique*).
- Estado del ticket: Registrado.

Registro de actividad de la etapa:

- Identificador del actor que ejecutó el registro (colaborador reportante o, en su defecto, Oficial de Soporte bajo registro asistido).
- Fecha y hora de cierre del registro.
- Bitácora de observaciones del registro.

Validaciones obligatorias aplicadas por la plataforma (ManageEngine ServiceDesk Plus). Con el propósito de garantizar que el ticket creado en ManageEngine ServiceDesk Plus contenga información mínima suficiente, trazable y útil para las etapas posteriores del flujo, la plataforma aplicará un conjunto de validaciones obligatorias antes de permitir el cierre del registro. Estas validaciones tienen carácter preventivo, debido a que buscan evitar registros incompletos, ambiguos, duplicados o carentes de evidencia suficiente. Las validaciones contempladas son las siguientes:

- **Obligatoriedad de los datos del reportante:** El ticket no podrá enviarse si no se encuentran completos los datos del colaborador reportante, su área y unidad organizacional, y su medio de contacto inicial.
- **Selección obligatoria del sistema afectado desde catálogo institucional:** El campo Sistema o aplicación afectada deberá seleccionarse del catálogo institucional parametrizado en la plataforma. No se admite ingreso de texto libre.
- **Selección obligatoria del módulo o funcionalidad desde catálogo institucional:** El campo Módulo o funcionalidad específica deberá seleccionarse del catálogo institucional asociado al sistema previamente elegido. No se admite ingreso de texto libre.
- **Estructura mínima de la descripción narrativa:** La Descripción narrativa de la incidencia deberá contener, como mínimo, el comportamiento esperado del sistema, el comportamiento observado por el reportante, la fecha aproximada de ocurrencia y el impacto percibido sobre la operación.
- **Evidencia obligatoria:** Cuando la incidencia involucre mensaje de error, bloqueo de operación, afectación a un proceso crítico o indisponibilidad de una funcionalidad, el sistema requerirá obligatoriamente la adjunción de evidencia, preferentemente de carácter visual (captura de pantalla, fotografía del mensaje de error o grabación del comportamiento observado).
- **Justificación obligatoria del registro asistido.** Cuando la modalidad de registro sea "Asistido por el Oficial", el campo *Justificación del registro asistido* se activará como obligatorio. En esa justificación deberá consignarse la imposibilidad técnica o

condición excepcional que impidió al colaborador efectuar el registro directo.

- **Advertencia de duplicidad inicial.** Antes de confirmar el registro, la plataforma advertirá al reportante sobre la existencia de tickets abiertos con coincidencia de reportante, sistema, módulo o descripción similar, a fin de prevenir registros duplicados y facilitar la vinculación con casos relacionados.
- **Inmutabilidad de los campos autogenerados.** El Identificador único del ticket, la Fecha y hora de registro y el Estado inicial "Registrado" son generados automáticamente por la plataforma y no son modificables por ningún actor del flujo.
- **Validación integral del estado inicial:** El ticket solo alcanzará el estado "Registrado" cuando la totalidad de las validaciones obligatorias anteriores haya sido cumplida. En caso contrario, permanecerá como borrador y no iniciará el cómputo formal del flujo de gestión.

Criterio de paso a la siguiente etapa. El ticket se considera apto para avanzar a la etapa de validación cuando todos los campos obligatorios se encuentran completados, la evidencia ha sido adjuntada en los casos que la requieran, y el identificador único ha sido generado por la plataforma y confirmado al reportante.

Tiempo objetivo asociado. El registro debe completarse de manera inmediata al momento de detectar la incidencia. El tiempo máximo aceptable para esta etapa será definido como parte del acuerdo de nivel de servicio aplicable, conforme a la matriz de criticidad desarrollada en el componente 6.4.3.

Regla de exclusividad del medio oficial. ManageEngine ServiceDesk Plus es el único medio oficial mediante el cual Banco FICENSA gestiona las incidencias de software de las áreas de Negocios y Operaciones. Ninguna incidencia se atiende, resuelve o cierra fuera de la plataforma institucional. Bajo el principio de autoservicio adoptado por el modelo, el registro de la incidencia es responsabilidad primaria del colaborador reportante. La intervención del Oficial de Soporte en el registro constituye una excepción aplicable únicamente bajo imposibilidad técnica documentada que impida al colaborador acceder al portal.

Etapa 1 — Registro

Modelo entrada – proceso – salida



Figura 21. Diagrama IPO, etapa 1

Fuente: Elaboración propia

6.4.2.2. ETAPA 2 - VALIDACIÓN

Propósito. Verificar que el ticket creado durante la Etapa 1 cumple con los estándares mínimos de calidad documental requeridos por el modelo institucional, antes de su clasificación y priorización. La validación constituye el primer punto de control de calidad dentro del flujo y representa la transición entre el registro efectuado por el colaborador y la gestión técnica del caso por parte del área de Tecnología y Comunicaciones. Su finalidad es garantizar que cada incidencia llegue a las etapas posteriores con información completa, coherente y suficiente para permitir un diagnóstico técnico efectivo, evitando con ello los reprocesos, las consultas reiteradas al reportante y las demoras innecesarias en la atención.

Evento disparador. Notificación automática generada por ManageEngine ServiceDesk Plus al Oficial de Soporte correspondiente, indicando que un nuevo ticket ha sido creado y se encuentra pendiente de validación. La notificación se emite de manera inmediata al cierre de la Etapa 1 y se enruta al Oficial de Soporte Proyectos / Help Desk como regla general o al Oficial de Soporte Cash Management cuando el ticket corresponde a ese sistema específico.

Actor responsable (R). Oficial de Soporte Proyectos / Help Desk para casos generales. Oficial de Soporte Cash Management para casos específicos del sistema Cash Management. El Oficial actúa en su rol de verificador de la calidad del registro y no como ejecutor de la atención técnica.

Actor aprobador (A). Jefe de Proyectos y Desarrollo, en su rol de coordinador táctico

del modelo y responsable del cumplimiento de los acuerdos de nivel de servicio del primer nivel. La etapa es ejecutada y cerrada por el Oficial de Soporte sin aprobación individual por cada ticket; el control del desempeño se ejerce mediante los indicadores del componente 6.5.

Actividades específicas:

- Acceder al ticket recién registrado en la plataforma a partir de la notificación automática recibida.
- Verificar la completitud de los campos obligatorios diligenciados durante la Etapa 1, contrastándolos con la lista institucional definida por el modelo.
- Evaluar la claridad de la descripción narrativa de la incidencia, confirmando que permite comprender de manera precisa el comportamiento del sistema afectado, el momento de ocurrencia y las condiciones operativas en que se manifestó.
- Revisar la suficiencia y pertinencia de la evidencia adjunta, comprobando que las capturas de pantalla, mensajes de error o documentos aportados respaldan adecuadamente lo descrito por el reportante.
- Identificar inconsistencias, omisiones o ambigüedades que requieran complementación por parte del colaborador.
- Emitir el dictamen de validación, conforme a uno de los dos resultados posibles del proceso.

En caso de que el ticket cumpla con los estándares de calidad documental, el Oficial actualiza el estado a "Validado" y libera el caso para la Etapa 3. En caso de que el ticket no cumpla, el Oficial actualiza el estado a "Devuelto al reportante", registra en la bitácora del ticket los motivos específicos de la devolución y notifica al colaborador para que complemente la información dentro del tiempo definido por el acuerdo de nivel de servicio aplicable. El ticket no avanza hasta que la complementación sea verificada nuevamente y obtenga el dictamen positivo.

Entrada. Ticket institucional creado durante la Etapa 1 en estado "Registrado", con sus campos obligatorios diligenciados y evidencia adjunta cuando el caso lo requiera.

Salida. Una de dos posibles, según el resultado del proceso de verificación. Como salida positiva, el ticket actualizado al estado "Validado", apto para avanzar a la Etapa 3 de clasificación.

Como salida negativa, el ticket actualizado al estado "Devuelto al reportante", con la bitácora actualizada con los motivos específicos de la devolución y la notificación enviada al colaborador para complementación.

Criterios objetivos de aceptación y rechazo del dictamen de validación. Con el propósito de eliminar la discrecionalidad en el dictamen emitido por el Oficial de Soporte y garantizar la reproducibilidad del proceso, el modelo formaliza un conjunto de criterios binarios que el Oficial deberá aplicar mediante verificación directa, mediante criterios verificables. Estos criterios complementan, en el plano de la calidad sustantiva, las validaciones automáticas de plataforma ya ejecutadas durante la Etapa 1, las cuales operan en el plano de la completitud formal. El dictamen "Validado" requiere el cumplimiento integral de los criterios de aceptación; la verificación de cualquiera de los criterios de rechazo determina el dictamen "Devuelto al reportante".

Tabla 37. Criterios objetivos de aceptación del dictamen de validación.

#	Criterio	Verificación directa por el Oficial de Soporte
CA-01	Coherencia interna del registro	La descripción narrativa, el sistema declarado, el módulo declarado y la evidencia adjunta se refieren al mismo evento operativo, sin contradicciones entre sí.
CA-02	Suficiencia descriptiva	La descripción narrativa contiene de forma identificable el comportamiento esperado, el comportamiento observado, el momento de ocurrencia y el impacto operativo percibido.
CA-03	Trazabilidad del reportante	Los datos del colaborador reportante permiten identificar inequívocamente al solicitante, su área y su unidad organizacional.
CA-04	Ámbito del modelo	El caso reportado constituye una incidencia de software de las áreas de Negocios u Operaciones.
CA-05	No duplicidad sustantiva	Tras revisar las advertencias de duplicidad generadas por la plataforma, el caso no corresponde a un ticket ya abierto; cuando exista relación con uno existente, se encuentra formalmente vinculado.
CA-06	Justificación del registro asistido	Cuando el ticket fue creado bajo la modalidad "Asistido por el Oficial", la justificación documentada describe una imposibilidad técnica verificable conforme a la regla de exclusividad del medio oficial.

Fuente: Elaboración propia.

Tabla 38. Criterios objetivos de devolución o rechazo del dictamen de validación.

#	Criterio	Verificación directa por el Oficial de Soporte
CR-01	Incoherencia interna del registro	Existe contradicción entre la descripción narrativa, el sistema declarado, el módulo declarado o la evidencia adjunta.
CR-02	Insuficiencia descriptiva	La descripción narrativa omite alguno de los cuatro elementos mínimos exigidos o se limita a expresiones genéricas que no permiten dimensionar el caso.
CR-03	Trazabilidad insuficiente del reportante	Los datos del colaborador reportante son incompletos, inconsistentes o no permiten identificar su área o unidad organizacional.
CR-04	Ámbito no aplicable	El caso no constituye una incidencia de software bajo el alcance del modelo, por corresponder a infraestructura, hardware, redes, soporte general al usuario, solicitud de servicio, requerimiento nuevo o cambio planificado.
CR-05	Duplicidad confirmada sin vinculación	El caso replica un ticket previamente abierto y no se ha efectuado la vinculación correspondiente. En este caso, el Oficial de Soporte deberá vincular el reporte al ticket activo, registrar la relación en la bitácora y notificar al reportante.
CR-06	Justificación inexistente o no verificable del registro asistido	La justificación del registro asistido es inexistente, genérica o no describe una imposibilidad técnica documentable.

Fuente: Elaboración propia.

Tiempos, responsables y puntos de control. Una vez definidos los criterios objetivos para emitir el dictamen de validación, la etapa requiere mecanismos de control que aseguren su aplicación oportuna, trazable y uniforme dentro del flujo operativo. Para ello, se establece un tiempo máximo de revisión, se delimitan las responsabilidades operativas y de supervisión, y se incorporan controles automáticos en ManageEngine ServiceDesk Plus orientados a evitar retrasos, registrar el resultado del dictamen y asegurar que las devoluciones al reportante cuenten con seguimiento documentado. Con esto, la validación se integra como un punto de control formal dentro del proceso, sin convertirse en una aprobación manual adicional.

Tabla 39. Tiempos, responsables y puntos de control etapa 2.

Tiempo máximo esperado	Responsable operativo	Responsable de aprobación/control	Punto de control automático propuesto en ServiceDesk Plus
30 minutos hábiles (uniforme para todos los niveles)	Oficial de Soporte Help Desk u Oficial Cash Management según el sistema afectado	No aplica aprobación individual. El Jefe de Proyectos y Desarrollo ejerce supervisión del desempeño general mediante los indicadores.	Detectivos: Alerta automática por proximidad de vencimiento del SLA de validación. Correctivos automáticos: Retorno automático del ticket al estado "Devuelto al

Tiempo máximo esperado	Responsable operativo	Responsable de aprobación/control	Punto de control automático propuesto en ServiceDesk Plus
			reportante" con bitácora cuando el dictamen es negativo; cierre automático por desistimiento si el reportante no complementa dentro del plazo. De trazabilidad: Bitácora automática del dictamen y del Oficial que lo emite.

Fuente: Elaboración propia.

Campos del ticket actualizados en esta etapa (ManageEngine ServiceDesk Plus):

- Dictamen de validación: Validado o Devuelto al reportante.
- Motivos específicos de la devolución (cuando aplique).
- Identificador de la versión validada del ticket, para fines de trazabilidad ante eventuales complementaciones.
- Estado del ticket: Validado o Devuelto al reportante, según corresponda.

Registro de actividades de la etapa (ManageEngine ServiceDesk Plus):

- Identificador del Oficial de Soporte que ejecutó la validación.
- Fecha y hora de cierre de la validación.
- Bitácora de observaciones de la validación

Criterio de paso a la siguiente etapa. El ticket se considera apto para avanzar a la Etapa 3 de clasificación cuando ha obtenido el dictamen "Validado" por parte del Oficial de Soporte, la bitácora de validación se encuentra completada y el estado del ticket en la plataforma ha sido actualizado en consecuencia. En el caso de los tickets devueltos al reportante, el avance solo procederá una vez que la complementación haya sido recibida y verificada en una nueva iteración de validación con dictamen positivo.

Tiempo objetivo asociado. La validación deberá ejecutarse dentro del tiempo máximo definido por el acuerdo de nivel de servicio aplicable a la criticidad estimada del caso, conforme a

la matriz desarrollada en el componente 6.4.3. La velocidad de validación es un factor crítico del modelo, dado que esta etapa precede la asignación técnica y, por tanto, condiciona el cumplimiento global del SLA del caso.

Regla de la doble vía y prevención del cuello de botella. La validación contempla únicamente dos resultados posibles, sin estados intermedios ni dictámenes condicionales. Esta regla evita que los tickets permanezcan indefinidamente en una zona gris de revisión y obliga al Oficial a emitir un dictamen claro dentro del tiempo objetivo. Cuando el ticket sea devuelto al reportante, la responsabilidad sobre el caso retorna al colaborador, quien dispone de un plazo definido para complementar la información requerida. Si la complementación no se recibe dentro del plazo, el ticket podrá ser cerrado por desistimiento del reportante, lo cual quedará documentado en la bitácora y reportado en los indicadores de seguimiento del modelo.

Etapa 2 — Validación
Modelo entrada – proceso – salida



Figura 22. Diagrama IPO, etapa 2

Fuente: Elaboración propia

6.4.2.3. ETAPA 3 – CLASIFICACIÓN

Propósito. Categorizar formalmente la incidencia validada conforme a las dimensiones institucionales definidas por el modelo, con el fin de habilitar su posterior priorización, asignación y análisis estadístico. La clasificación constituye el primer acto de inteligencia organizacional sobre el caso, dado que transforma una descripción narrativa libre en información estructurada susceptible de medición, comparación histórica y detección de patrones. Su finalidad es garantizar que cada incidencia quede tipificada bajo categorías homogéneas que permitan, en el corto plazo, una asignación técnica precisa y, en el mediano plazo, la identificación de tendencias recurrentes

que alimenten la práctica de Gestión de Problemas.

Evento disparador. Actualización del estado del ticket a "Validado" como resultado de la Etapa 2, que habilita la apertura del formulario de clasificación dentro de ManageEngine ServiceDesk Plus. La notificación se enruta automáticamente al Oficial de Soporte responsable del caso.

Actor responsable (R). Oficial de Soporte Proyectos / Help Desk para casos generales. Oficial de Soporte Cash Management para casos específicos del sistema Cash Management. El Oficial actúa en su rol de clasificador especializado, aplicando los criterios taxonómicos institucionales conforme a la información contenida en el ticket validado.

Actor aprobador (A). Jefe de Proyectos y Desarrollo, en su carácter de coordinador táctico del modelo y responsable de la consistencia taxonómica del proceso a lo largo del tiempo.

Actividades específicas:

- Acceder al ticket en estado "Validado" a partir de la notificación automática recibida.
- Asignar el tipo de incidencia conforme a la taxonomía institucional, distinguiendo entre incidencia funcional (error o comportamiento inesperado del software), incidencia de disponibilidad (interrupción total o parcial del servicio), incidencia de desempeño (degradación de tiempos de respuesta) o incidencia de seguridad (compromiso o sospecha de compromiso de la integridad del sistema).
- Confirmar o ajustar el sistema o aplicación afectada, verificando que el dato registrado por el reportante corresponda al sistema realmente involucrado en la falla, y precisar el módulo específico cuando el reporte inicial haya sido genérico.
- Asignar el área funcional impactada, distinguiendo entre Negocios, Operaciones o ambas, conforme al alcance organizacional de la afectación.
- Identificar si el caso corresponde a una incidencia individual o si guarda relación con tickets previos del mismo reportante, sistema o módulo, vinculándolos en la plataforma cuando proceda para fines de trazabilidad histórica.
- Registrar la clasificación en los campos correspondientes del ticket y actualizar el estado a "Clasificado", habilitando con ello el cálculo automático de la prioridad en la Etapa 4.

Entrada. Ticket institucional en estado "Validado", proveniente de la Etapa 2, con la información del reportante, sistema afectado, módulo y descripción narrativa confirmada como completa, clara y suficiente.

Salida. Ticket institucional actualizado al estado "Clasificado", con las dimensiones taxonómicas debidamente asignadas (tipo de incidencia, sistema afectado, módulo específico, área funcional impactada y vínculos con tickets relacionados cuando aplique), apto para el cálculo automático de la prioridad en la Etapa 4.

Tabla 40. Tiempos, responsables y puntos de control etapa 3.

Tiempo máximo esperado	Responsable operativo	Responsable de aprobación/control	Punto de control automático propuesto en ServiceDesk Plus
20 minutos hábiles (uniforme para todos los niveles)	Oficial de Soporte Help Desk u Oficial Cash Management	Jefe de Proyectos y Desarrollo, responsable de la consistencia taxonómica del proceso a lo largo del tiempo.	Preventivos: Lista obligatoria de tipo de incidencia, sistema afectado, módulo y área funcional; alerta de clasificación incompleta antes de avanzar a priorización. Detectivos: Vinculación automática con tickets previos del mismo sistema o módulo para detección de duplicidad o reincidencia.

Fuente: Elaboración propia.

Campos del ticket actualizados en esta etapa (ManageEngine ServiceDesk Plus):

- Tipo de incidencia: Funcional, Disponibilidad, Desempeño o Seguridad.
- Sistema o aplicación afectada confirmada o ajustada por el Oficial.
- Módulo o funcionalidad específica precisada por el Oficial.
- Área funcional impactada: Negocios, Operaciones o Ambas.
- Vínculo con tickets previos relacionados (*cuando aplique*).
- Estado del ticket: Clasificado.

Registro de actividades de la etapa (ManageEngine ServiceDesk Plus):

- Identificador del Oficial de Soporte que ejecutó la clasificación.

- Fecha y hora de cierre de la clasificación.
- Bitácora de observaciones de la clasificación

Criterio de paso a la siguiente etapa. El ticket se considera apto para avanzar a la Etapa 4 de priorización cuando todas las dimensiones taxonómicas obligatorias han sido asignadas, los vínculos con tickets relacionados han sido registrados en los casos que correspondan, y el estado del ticket en la plataforma ha sido actualizado a "Clasificado".

Tiempo objetivo asociado. La clasificación deberá ejecutarse dentro del tiempo máximo definido por el acuerdo de nivel de servicio aplicable a la criticidad estimada del caso, conforme a la matriz desarrollada en el componente 6.4.3. Por tratarse de una etapa esencialmente cognitiva y no operativa, su duración debe ser breve y consecutiva a la validación.

Importancia de la consistencia taxonómica. La calidad del modelo a lo largo del tiempo depende de la consistencia con la cual se aplican las categorías de clasificación. Una taxonomía aplicada de manera inconsistente genera datos no comparables, distorsiona los indicadores de seguimiento e impide identificar correctamente los patrones de reincidencia que alimentan la práctica de Gestión de Problemas. Por esta razón, el modelo asigna al Jefe de Proyectos y Desarrollo la responsabilidad de revisar periódicamente la coherencia de las clasificaciones efectuadas y, cuando corresponda, de promover ajustes formales a la taxonomía institucional ante cambios tecnológicos o regulatorios que lo justifiquen.

Catálogo institucional de categorías y subcategorías para la clasificación de incidencias de software. Conforme a la práctica de Gestión de Incidentes de ITIL 4, la categorización constituye una actividad sustantiva del ciclo de vida del incidente y debe ejecutarse contra un catálogo institucional cerrado, parametrizado en la plataforma y mantenido por la autoridad técnica del proceso (AXELOS, 2019). El catálogo institucional propuesto se construye sobre tres principios.

Primero, dos niveles taxonómicos (categoría y subcategoría) para garantizar análisis a la vez agregado y granular.

Segundo, dependencia jerárquica controlada por la plataforma, conforme a la cual la selección de la subcategoría depende de la categoría previamente elegida, y la selección del módulo depende del sistema previamente confirmado.

Tercero, mecanismo de captura residual gobernado, que admite valores tipo "Otro" únicamente bajo condiciones documentadas y sujetas a revisión periódica del catálogo, de modo que el modelo aprenda de los casos no anticipados y el catálogo evolucione sin perder cierre operativo. El catálogo se compone de cuatro instrumentos taxonómicos: el catálogo de Tipo de Incidencia (CAT A), el catálogo de Sistemas afectados (CAT B), el catálogo de Módulos (de dependencia paramétrica), y el catálogo de Vínculos con tickets previos (CAT C).

Tabla 41. CAT A. Catálogo oficial de Tipo de Incidencia.

Código categoría	Categoría (nivel 1)	Código subcategoría	Subcategoría (nivel 2)	Definición operativa
TI-FUN	Funcional	TI-FUN-01	Falla funcional	El sistema no permite ejecutar una operación esperada o produce un resultado incompleto.
TI-FUN	Funcional	TI-FUN-02	Error puntual	El sistema emite un mensaje de error específico, reproducible, sobre una operación concreta.
TI-FUN	Funcional	TI-FUN-03	Datos incorrectos	La información generada, procesada o desplegada por el sistema es errónea.
TI-FUN	Funcional	TI-FUN-99	Otro funcional	Caso de naturaleza funcional no contemplado en las subcategorías anteriores; obliga a descripción extendida.
TI-DSP	Disponibilidad	TI-DSP-01	Caída total del sistema	Indisponibilidad completa del sistema o aplicación.
TI-DSP	Disponibilidad	TI-DSP-02	Caída parcial	Indisponibilidad de uno o varios módulos manteniendo el resto operativo.
TI-DSP	Disponibilidad	TI-DSP-03	Bloqueo por credenciales o sesión	Imposibilidad de acceso por causa de credenciales, sesión o permisos.
TI-DSP	Disponibilidad	TI-DSP-99	Otro de disponibilidad	Caso de disponibilidad no contemplado; obliga a descripción extendida.
TI-DES	Desempeño	TI-DES-01	Lentitud	Tiempos de respuesta degradados, manteniendo operatividad.
TI-DES	Desempeño	TI-DES-02	Timeout	La operación excede el límite de tiempo y se interrumpe sin completar.
TI-DES	Desempeño	TI-DES-99	Otro de desempeño	Caso de desempeño no contemplado; obliga a descripción extendida.
TI-INT	Integración	TI-INT-01	Falla de	Interrupción del intercambio de datos entre

Código categoría	Categoría (nivel 1)	Código subcategoría	Subcategoría (nivel 2)	Definición operativa
			comunicación con sistemas internos	sistemas del banco.
TI-INT	Integración	TI-INT-02	Falla de comunicación con sistemas externos	Interrupción del intercambio con proveedores, entes regulatorios o terceros.
TI-INT	Integración	TI-INT-03	Inconsistencia o desincronización de datos	Los sistemas integrados presentan información divergente sobre una misma transacción o registro.
TI-INT	Integración	TI-INT-99	Otro de integración	Caso de integración no contemplado; obliga a descripción extendida.
TI-SEG	Seguridad	TI-SEG-01	Acceso no autorizado	Acceso, sospechado o confirmado, sin las autorizaciones correspondientes.
TI-SEG	Seguridad	TI-SEG-02	Compromiso de credenciales	Sospecha o confirmación de divulgación, sustracción o uso indebido de credenciales.
TI-SEG	Seguridad	TI-SEG-03	Modificación o eliminación indebida de datos	Alteración o supresión no autorizada de registros del sistema.
TI-SEG	Seguridad	TI-SEG-99	Otro de seguridad	Caso de seguridad no contemplado; obliga a descripción extendida y notificación inmediata al área de Seguridad de la Información.
TI-NCL	No clasificable	TI-NCL-00	Pendiente de tipificación	El caso no admite asignación a ninguna categoría existente al momento de la clasificación; obliga a escalamiento al Jefe de Proyectos y Desarrollo para tipificación dentro de 24 horas hábiles.

Fuente: Elaboración propia con base en ITIL 4 (AXELOS, 2019) y en la taxonomía operativa del Capítulo IV.

Tabla 42. CAT B. Catálogo institucional inicial de sistemas afectados.

Código	Sistema	Marca de criticidad	Origen del reconocimiento
SIS-01	Inclusión Financiera	Crítico	Recurrencia identificada en el Capítulo IV
SIS-02	ENEE	Crítico	Recurrencia identificada en el Capítulo IV
SIS-03	RAP	Crítico	Recurrencia identificada en el Capítulo IV
SIS-04	Conciliación SINAP	Crítico	Recurrencia identificada en el Capítulo IV
SIS-05	Instituto de la propiedad	Crítico	Categorizado en crítico por las implicaciones de pérdidas monetarias y reputacionales.
SIS-06	AMDC	Crítico	Categorizado en crítico por las implicaciones de pérdidas monetarias y reputacionales.
SIS-07	AMSPS	Crítico	Categorizado en crítico por las implicaciones de pérdidas monetarias y reputacionales.
SIS-08	Cash Management	Estándar	Sistema bajo dominio operativo del Oficial Cash Management
SIS-09	Integración Hubspot	Estándar	Sistema bajo dominio operativo del Oficial Cash Management
SIS-09 a SIS-NN	Sistemas restantes del portafolio institucional	Estándar	Parametrización progresiva por la Gerencia de Tecnología y Comunicaciones
SIS-99	Otro sistema	Estándar	Captura residual; obliga a descripción del sistema y activa propuesta de incorporación al catálogo

Fuente: Elaboración propia.

Tabla 43. CAT C. Catálogo de Tipos de vínculo con tickets previos.

Código	Tipo de vínculo	Definición operativa
VIN-00	Sin vínculo	El caso no guarda relación identificable con tickets previos.
VIN-01	Relacionado	El caso involucra el mismo sistema o módulo de un ticket previo, pero constituye un evento distinto.
VIN-02	Duplicado	El caso replica un ticket actualmente abierto; se vincula y se cierra por duplicidad.
VIN-03	Recurrente	El caso replica un ticket previamente cerrado que vuelve a presentarse; activa marca de candidato a Gestión de Problemas.

Fuente: Elaboración propia.

Etapa 3 — Clasificación

Modelo entrada – proceso – salida

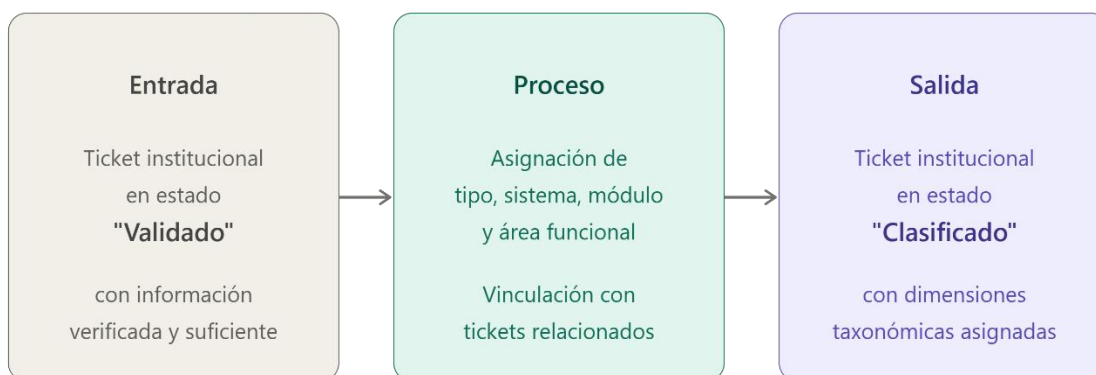


Figura 23. Diagrama IPO, etapa 3

Fuente: Elaboración propia.

6.4.2.4.ETAPA 4 – PRIORIZACIÓN

Propósito. Asignar al ticket clasificado el nivel de prioridad institucional que regirá los tiempos de atención y resolución del caso, mediante el cruce sistemático del impacto operativo y la urgencia técnica conforme a la matriz de criticidad institucional. La priorización constituye el acto que traduce la clasificación taxonómica de la etapa anterior en un compromiso temporal medible, dando inicio al cómputo del acuerdo de nivel de servicio aplicable al caso. Su finalidad es garantizar que cada incidencia reciba un nivel de atención proporcional al daño operativo que produce, evitando la sobre-reacción ante casos menores y la sub-reacción ante casos críticos identificada durante el diagnóstico.

Evento disparador. Actualización del estado del ticket a "Clasificado" como resultado

de la Etapa 3, que habilita la apertura del cálculo automático de prioridad dentro de ManageEngine ServiceDesk Plus. El cálculo se ejecuta de manera inmediata sobre las dimensiones taxonómicas previamente asignadas.

Actor responsable (R). Oficial de Soporte Proyectos / Help Desk para casos generales. Oficial de Soporte Cash Management para casos específicos del sistema Cash Management. El Oficial actúa como evaluador de las variables de impacto y urgencia y como validador del nivel de prioridad calculado por el sistema.

Actor aprobador (A). Jefe de Proyectos y Desarrollo, quien autoriza los ajustes manuales de prioridad cuando proceda y supervisa la consistencia de la priorización a lo largo del tiempo.

Actividades específicas:

- Acceder al ticket en estado "Clasificado" a partir de la notificación automática recibida.
- Determinar el nivel de impacto operativo del caso considerando el alcance organizacional de la afectación (cantidad de colaboradores, unidades o áreas afectadas), el grado de degradación del servicio y la criticidad regulatoria del proceso interrumpido.
- Determinar el nivel de urgencia técnica del caso considerando la disponibilidad de soluciones alternativas, la ventana temporal del proceso afectado y la proximidad de obligaciones regulatorias o transaccionales asociadas.
- Verificar el nivel de prioridad calculado de manera automática por el motor de la plataforma a partir del cruce de impacto y urgencia conforme a la matriz de criticidad institucional definida en el componente 6.4.3.
- Confirmar el nivel de prioridad asignado o, cuando se justifique técnicamente, solicitar al Jefe de Proyectos y Desarrollo un ajuste manual debidamente documentado en la bitácora del ticket.
- Activar formalmente el acuerdo de nivel de servicio correspondiente al nivel de prioridad confirmado y actualizar el estado del ticket a "Priorizado".

Entrada. Ticket institucional en estado "Clasificado", proveniente de la Etapa 3, con las dimensiones taxonómicas asignadas (tipo de incidencia, sistema afectado, módulo específico, área

funcional impactada y vínculos con tickets relacionados cuando aplique).

Salida. Ticket institucional actualizado al estado "Priorizado", con el nivel de prioridad confirmado, el acuerdo de nivel de servicio activado y los tiempos objetivo de las etapas posteriores debidamente calculados y visibles en la plataforma.

Tabla 44. Tiempos, responsables y puntos de control etapa 4.

Tiempo máximo esperado	Responsable operativo	Responsable de aprobación/control	Punto de control automático propuesto en ServiceDesk Plus
Crítica: 15 min; Alta: 1 h hábil; Media: 2 h hábiles; Baja: 4 h hábiles; Planificada: programada	Oficial de Soporte Help Desk u Oficial Cash Management	Jefe de Proyectos y Desarrollo, únicamente en los ajustes manuales de prioridad debidamente justificados, conforme a la regla del ajuste manual excepcional.	Preventivos: cálculo automático del nivel de prioridad mediante cruce impacto × urgencia; aplicación automática del agravamiento por sistema crítico (Inclusión Financiera, ENEE, RAP, Conciliación SINAP). Detectivos: alerta automática si la priorización excede su tiempo máximo. Correctivos automáticos: activación automática del SLA correspondiente al confirmar la prioridad.

Fuente: Elaboración propia.

Campos del ticket actualizados en esta etapa (ManageEngine ServiceDesk Plus):

- Nivel de impacto operativo evaluado: Alto, Medio o Bajo.
- Nivel de urgencia técnica evaluada: Alta, Media o Baja.
- Nivel de prioridad calculado automáticamente por la matriz institucional: Crítica, Alta, Media, Baja o Planificada.
- Modalidad de prioridad: Confirmada o Ajustada manualmente.
- Nivel de prioridad final confirmado.
- Justificación del ajuste manual de prioridad (*cuando aplique*).
- Identificador del Jefe de Proyectos y Desarrollo que autorizó el ajuste manual (*cuando aplique*).

- Identificador del acuerdo de nivel de servicio activado, con sus tiempos objetivo aplicables a las etapas posteriores.
- Estado del ticket: Priorizado.

Registro de actividades de la etapa (ManageEngine ServiceDesk Plus):

- Identificador del Oficial de Soporte que ejecutó la priorización.
- Fecha y hora de cierre de la priorización.
- Bitácora de observaciones de la priorización.

Criterio de paso a la siguiente etapa. El ticket se considera apto para avanzar a la Etapa 5 de asignación cuando el nivel de prioridad ha sido confirmado conforme a la matriz de criticidad institucional, el acuerdo de nivel de servicio ha sido activado en la plataforma, los tiempos objetivo de las etapas posteriores han quedado calculados y visibles, y el estado del ticket en la plataforma ha sido actualizado a "Priorizado".



Figura 24. Evaluación del impacto operativo.

Fuente: Elaboración propia.

La figura presenta los niveles de impacto operativo utilizados en la Etapa 4 para

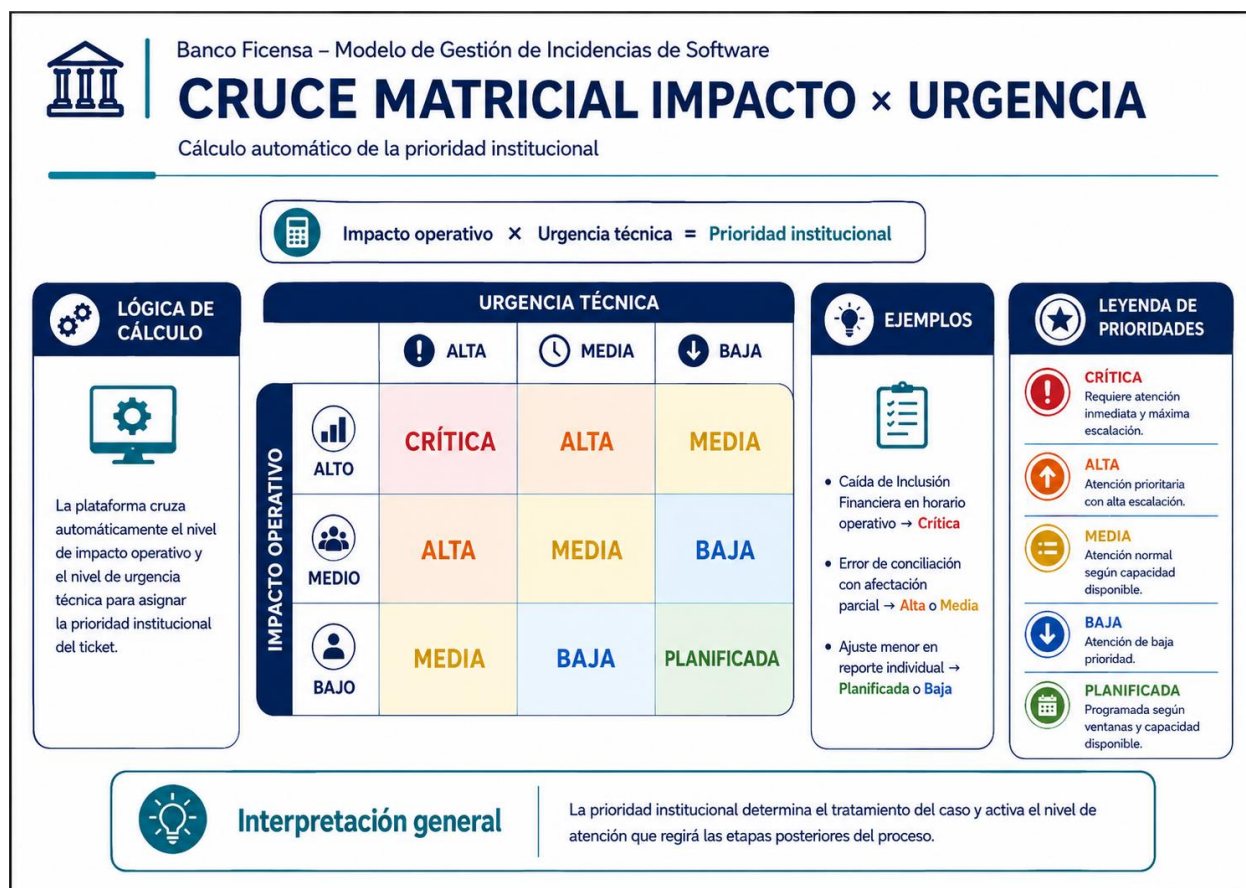
determinar el grado de afectación que una incidencia de software genera sobre la operación bancaria. Esta evaluación distingue entre impacto alto, medio y bajo, considerando criterios como interrupción de procesos críticos, afectación a múltiples usuarios, existencia de alternativas operativas y riesgo regulatorio, financiero o reputacional.



Figura 25. Evaluación de la urgencia técnica.

Fuente: Elaboración propia.

La figura muestra los niveles de urgencia técnica aplicables a las incidencias de software, diferenciando entre urgencia alta, media y baja según la rapidez requerida para intervenir el caso. Esta valoración permite establecer si la incidencia demanda atención inmediata, atención en el corto plazo o una respuesta programable, tomando en cuenta el riesgo de demora, la posibilidad de interrupción prolongada y la existencia de medidas temporales.





AGRAVAMIENTO POR SISTEMA CRÍTICO

Aplicable cuando el sistema afectado pertenece al catálogo crítico institucional.



Regla de agravamiento

Si el sistema afectado pertenece al catálogo crítico y la prioridad calculada es Media, Baja o Planificada, la plataforma eleva automáticamente la prioridad un nivel. Si la prioridad calculada es Crítica o Alta, se mantiene sin cambio.

Conversión automática

Prioridad calculada		Prioridad final
Media	→	Alta
Baja	→	Media
Planificada	→	Baja
Alta	→	Alta
Crítica	→	Crítica



Activación del SLA

El SLA correspondiente al nivel final se activa inmediatamente y rige las Etapas 5, 6 y 7 del proceso: Asignación, Diagnóstico y Resolución, y Validación del Usuario y Cierre Formal.



Interpretación general

El agravamiento por sistema crítico protege la continuidad operativa de los servicios bancarios esenciales y asegura un tratamiento proporcional al riesgo del negocio.

Figura 27. Agravamiento por sistema crítico y activación del SLA.

Fuente: Elaboración propia.

La figura resume la lógica mediante la cual el modelo eleva automáticamente la prioridad de una incidencia cuando el sistema afectado pertenece al catálogo crítico institucional. Esta regla permite que casos inicialmente clasificados como media, baja o planificada reciban un tratamiento más exigente, activando el SLA correspondiente al nivel final de prioridad y fortaleciendo la continuidad operativa de los servicios bancarios esenciales.

Tiempo objetivo asociado. La priorización deberá ejecutarse de manera consecutiva a la clasificación, dentro de un tiempo máximo breve definido por el acuerdo de nivel de servicio aplicable a la criticidad estimada del caso. Por tratarse de una etapa cuyo retraso afecta directamente la totalidad de los tiempos posteriores, su cumplimiento es especialmente crítico para el desempeño global del modelo.

Regla del ajuste manual excepcional. El nivel de prioridad calculado de manera automática por la matriz institucional constituye la regla general del modelo y debe ser respetado

en todos los casos en que no exista una justificación técnica que amerite su ajuste. Sin embargo, el modelo contempla la posibilidad de un ajuste manual cuando concurren circunstancias específicas no previstas por la matriz, tales como obligaciones regulatorias inminentes, riesgos reputacionales identificados, situaciones de continuidad operativa que requieran tratamiento preferente o decisiones gerenciales debidamente comunicadas. Todo ajuste manual deberá ser solicitado por el Oficial de Soporte, autorizado por el Jefe de Proyectos y Desarrollo y documentado en la bitácora del ticket con la justificación correspondiente. Esta regla evita la discrecionalidad arbitraria y, al mismo tiempo, preserva la flexibilidad institucional necesaria para situaciones extraordinarias.

Etapa 4 — Priorización

Modelo entrada – proceso – salida

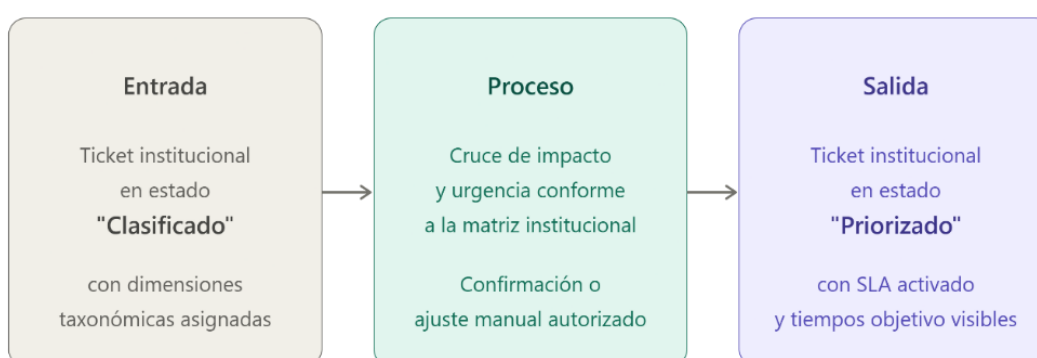


Figura 28. Diagrama IPO, etapa 4

Fuente: Elaboración propia.

6.4.2.5. ETAPA 5 – ASIGNACIÓN

Propósito. Determinar el actor técnico responsable de ejecutar las etapas siguientes del flujo a partir del nivel de prioridad confirmado y el sistema afectado, mediante la aplicación de reglas institucionales de enrutamiento que garanticen una distribución eficiente de la carga técnica y un balance adecuado entre especialización y disponibilidad. La asignación constituye el acto que conecta la decisión de gestión del primer nivel con la ejecución técnica del segundo nivel, transfiriendo formalmente la titularidad operativa del ticket al actor que asumirá su diagnóstico y resolución. Su finalidad es eliminar la ambigüedad en la atribución de responsabilidades técnicas identificada durante el diagnóstico y garantizar que cada caso sea atendido por el perfil profesional

adecuado a su complejidad.

Evento disparador. Actualización del estado del ticket a "Priorizado" como resultado de la Etapa 4, con el acuerdo de nivel de servicio activado y los tiempos objetivo de las etapas posteriores debidamente calculados. La notificación se enruta automáticamente al Oficial de Soporte responsable del caso.

Actor responsable (R). Oficial de Soporte Proyectos / Help Desk para casos generales. Oficial de Soporte Cash Management para casos específicos del sistema Cash Management. El Oficial aplica las reglas institucionales de enrutamiento y formaliza la asignación al técnico de segundo nivel correspondiente.

Actor aprobador (A). Jefe de Proyectos y Desarrollo, quien autoriza las reasignaciones excepcionales y supervisa la distribución equilibrada de la carga técnica entre los analistas programadores del segundo nivel.

Tabla 45. Tiempos, responsables y puntos de control etapa 5.

Tiempo máximo esperado	Responsable operativo	Responsable de aprobación/control	Punto de control automático propuesto en ServiceDesk Plus
Crítica: 15 min; Alta: 1 h hábil; Media: 2 h hábiles; Baja: 4 h hábiles; Planificada: programada	Oficial de Soporte Help Desk u Oficial Cash Management	Jefe de Proyectos y Desarrollo, únicamente en las reasignaciones manuales que se aparten de la regla institucional de enrutamiento.	Preventivos: Enrutamiento automático por nivel de prioridad (Crítica/Alta asignada a Senior Media/Baja asignada a Junior con menor carga). Detectivos: Alerta automática por ticket sin responsable técnico asignado. De Trazabilidad: Notificación automática al técnico asignado; Cómputo automático de la carga operativa de cada técnico.

Fuente: Elaboración propia.

Actividades específicas:

- Acceder al ticket en estado "Priorizado" a partir de la notificación automática recibida.
- Evaluar la concurrencia de variables de enrutamiento: nivel de prioridad confirmado, tipo

de incidencia, sistema afectado y módulo específico.

- Aplicar las reglas institucionales de enrutamiento, conforme a las cuales los casos de nivel de prioridad Crítica o Alta se asignan al Analista Programador Senior por razones de especialización, los casos de nivel de prioridad Media o Baja se distribuyen entre los Analistas Programador Junior conforme a su disponibilidad operativa, y los casos de nivel Planificada se incorporan a la cola de gestión programada del área.
- Verificar la disponibilidad operativa del técnico identificado, considerando su carga actual de tickets activos y la ventana temporal exigida por el acuerdo de nivel de servicio.
- Formalizar la asignación en la plataforma, transfiriendo la titularidad operativa del ticket al técnico designado y notificándole de manera automática la nueva responsabilidad.
- Actualizar el estado del ticket a "Asignado" y dejar constancia de la regla de enrutamiento aplicada.

En los casos excepcionales en los que la regla automática de enrutamiento no resulte aplicable o conduzca a una asignación inviable, el Oficial de Soporte solicita al Jefe de Proyectos y Desarrollo una reasignación manual autorizada, justificada en la bitácora del ticket. Esta excepción opera bajo el mismo principio de control aplicado en la Etapa 4, preservando la disciplina del modelo sin sacrificar la flexibilidad institucional necesaria.

Entrada. Ticket institucional en estado "Priorizado", proveniente de la Etapa 4, con el nivel de prioridad confirmado, el acuerdo de nivel de servicio activado y los tiempos objetivo de las etapas posteriores debidamente calculados y visibles en la plataforma.

Salida. Ticket institucional actualizado al estado "Asignado", con la titularidad operativa transferida al técnico de segundo nivel designado, la regla de enrutamiento aplicada debidamente documentada y la notificación al técnico emitida por la plataforma.

Campos del ticket actualizados en esta etapa (ManageEngine ServiceDesk Plus):

- Regla de enrutamiento aplicada (automática conforme al nivel de prioridad y al sistema afectado, o reasignación manual autorizada).
- Identificador del técnico de segundo nivel asignado: Analista Programador Senior o Analista Programador Junior.

- Carga operativa del técnico al momento de la asignación (*número de tickets activos*).
- Modalidad de asignación: Automática o Reasignación manual autorizada.
- Justificación de la reasignación manual (*cuando aplique*).
- Identificador del Jefe de Proyectos y Desarrollo que autorizó la reasignación manual (*cuando aplique*).
- Estado del ticket: Asignado.

Registro de actividades de la etapa (ManageEngine ServiceDesk Plus):

- Identificador del Oficial de Soporte que ejecutó la asignación.
- Fecha y hora de cierre de la asignación.
- Bitácora de observaciones de la asignación.

Criterio de paso a la siguiente etapa. El ticket se considera apto para avanzar a la Etapa 6 de diagnóstico cuando la regla de enrutamiento ha sido aplicada y documentada, el técnico de segundo nivel ha sido formalmente designado, la titularidad operativa ha sido transferida en la plataforma, el técnico ha recibido la notificación automática correspondiente y el estado del ticket ha sido actualizado a "Asignado".

Tiempo objetivo asociado. La asignación deberá ejecutarse de manera consecutiva a la priorización, dentro de un tiempo máximo breve definido por el acuerdo de nivel de servicio aplicable a la prioridad del caso. Por tratarse de una etapa cuyo retraso afecta directamente el tiempo total de atención percibido por el usuario y reduce la ventana técnica disponible para el segundo nivel, su cumplimiento puntual es un factor crítico del modelo.

Regla institucional de enrutamiento. El modelo adopta una regla de enrutamiento técnica fundamentada en el nivel de prioridad confirmado durante la Etapa 4, conforme a la siguiente lógica institucional:

Tabla 46. Niveles de prioridad.

Nivel de prioridad	Técnico asignado	Justificación
Crítica	Analista Programador Senior	Casos de máximo impacto operativo que exigen el mayor nivel de especialización técnica disponible en el banco.
Alta	Analista Programador Senior	Casos de alto impacto que requieren resolución especializada en tiempos comprimidos.

Nivel de prioridad	Técnico asignado	Justificación
Media	Analista Programador Junior (distribución por disponibilidad)	Casos de impacto moderado que pueden ser resueltos con el perfil técnico estándar.
Baja	Analista Programador Junior (distribución por disponibilidad)	Casos de impacto bajo que admiten tiempos extendidos de atención.
Planificada	Cola de gestión programada del área	Casos sin urgencia inmediata que se incorporan al cronograma técnico ordinario.

Fuente: Elaboración propia.

La distribución entre los tres Analistas Programador Junior se efectúa conforme a la carga operativa de cada uno al momento de la asignación, priorizando al técnico con menor número de tickets activos. Esta regla evita la concentración de carga sobre un único técnico y promueve un balance operativo sostenible.

Mecanismos automáticos de reasignación. La regla institucional de enrutamiento define la asignación inicial del ticket, pero el modelo reconoce que las condiciones operativas del segundo nivel técnico pueden variar entre el momento de la asignación y el inicio efectivo de la atención.

Para preservar el cumplimiento del acuerdo de nivel de servicio sin depender de la intervención manual sistemática del Jefe de Proyectos y Desarrollo, el modelo establece un conjunto de mecanismos automáticos de reasignación que ManageEngine ServiceDesk Plus ejecuta cuando se verifican condiciones objetivas predefinidas. Estos mecanismos operan dentro de los límites del catálogo de roles técnicos institucionales y no alteran la lógica del enrutamiento primario, sino que la corrigen ante desviaciones operativas detectables sin participación humana en el disparador. Cada activación queda registrada en la bitácora del ticket con el código del mecanismo aplicado, el técnico originalmente asignado, el técnico final y el motivo automático correspondiente, conforme al principio de trazabilidad institucional adoptado por el modelo.

Los mecanismos contemplados se presentan a continuación, ordenados según el momento del ciclo operativo en que pueden activarse.

Tabla 47. Mecanismos automáticos de reasignación de la Etapa 5.

Código	Mecanismo	Disparador automático detectado por la plataforma	Acción automática	Destino del ticket
MR-01	Reasignación por indisponibilidad	Marca de "no disponible" del técnico designado en el calendario institucional	Reenrutamiento automático y notificación al analista	Analista del mismo perfil con menor carga operativa

Código	Mecanismo	Disparador automático detectado por la plataforma	Acción automática	Destino del ticket
	del técnico	(vacaciones, permiso, ausencia justificada o estado fuera de línea durante jornada hábil) al momento de la asignación o durante su vigencia.	de respaldo	
MR-02	Reasignación por saturación operativa	Técnico designado con carga operativa activa superior al umbral parametrizado por la Gerencia de Tecnología y Comunicaciones.	Reenrutamiento automático conforme a la disponibilidad observada en la plataforma	Analista del mismo nivel con menor carga. Escalamiento al Analista Programador Senior si ningún Junior tiene capacidad
MR-03a	Reasignación por no aceptación del ticket	Ticket sin transición al estado "En atención" dentro del primer 10% del SLA técnico aplicable	Reenrutamiento automático y notificación informativa al Jefe de Proyectos y Desarrollo	Analista del mismo perfil con menor carga operativa
MR-03b	Reasignación por inactividad posterior a la aceptación	Ticket en estado "En atención" sin actualización de bitácora dentro del 25% del SLA técnico aplicable	Reenrutamiento automático y notificación obligatoria al Jefe de Proyectos y Desarrollo	Analista del mismo perfil con menor carga operativa
MR-04	Reasignación por reclasificación ascendente	Reclasificación del nivel de prioridad de Media o Baja a Alta o Crítica conforme a la Regla 2 de escalamiento del componente 6.4.3.3	Reenrutamiento automático al perfil técnico correspondiente al nuevo nivel	Analista Programador Senior
MR-05	Reasignación por horario no hábil para casos críticos	Ingreso o agravamiento de ticket Crítica fuera de la jornada laboral institucional	Enrutamiento al Analista Programador Senior disponible o a la cola crítica definida; si no existe disponibilidad registrada, notificación automática al Jefe de Proyectos y Desarrollo.	Analista designado en la guardia técnica institucional
MR-06	Reasignación por especialización de sistema	Sistema afectado con técnico especialista designado en el catálogo institucional de sistemas	Enrutamiento directo al especialista, omitiendo la distribución por carga operativa	Enrutamiento al técnico de segundo nivel especialista designado para el sistema afectado; cuando el sistema sea Cash Management, el Oficial CM conserva rol de validación operativa o coordinación, sin sustituir al técnico resolutor.

Fuente:

Elaboración

propia.

Nota: Para efectos del modelo, la guardia técnica institucional se entiende como el analista disponible o la cola crítica configurada para la atención de incidencias críticas fuera de la jornada laboral, sin implicar la creación de una nueva estructura organizativa.

Etapa 5 — Asignación

Modelo entrada – proceso – salida

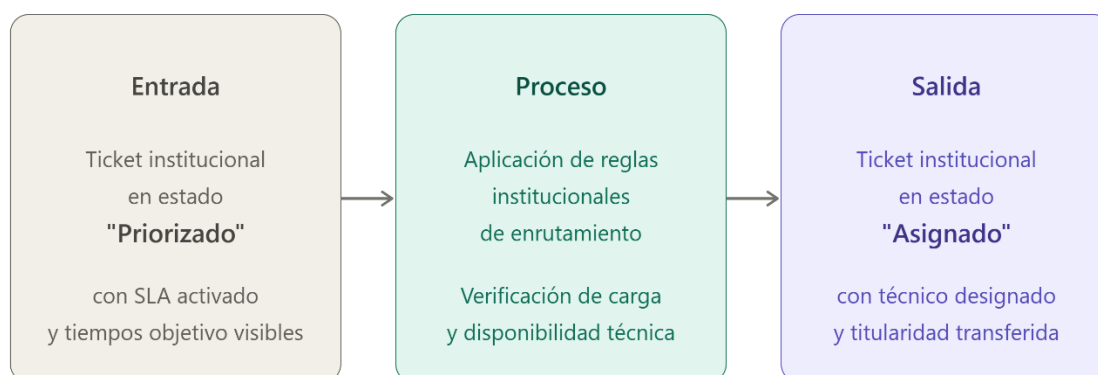


Figura 29. Diagrama IPO, etapa 5

Fuente: Elaboración propia.

6.4.2.6. ETAPA 6 - DIAGNÓSTICO Y RESOLUCIÓN

Propósito. Identificar la causa técnica de la incidencia asignada y aplicar la solución que restaura la operación normal del servicio dentro de los tiempos comprometidos por el acuerdo de nivel de servicio. La etapa de diagnóstico y resolución constituye el núcleo técnico del flujo, dado que es el momento en el cual el modelo produce valor tangible para el negocio: el sistema afectado vuelve a estar disponible para el colaborador y, con ello, para la operación bancaria. Su finalidad es garantizar que la atención técnica se ejecute bajo criterios uniformes de diagnóstico, documentación y aplicación de soluciones, eliminando las prácticas informales identificadas durante el diagnóstico y construyendo simultáneamente una base de conocimiento que reduzca la dependencia del modelo respecto del conocimiento tácito de los técnicos.

Evento disparador. Actualización del estado del ticket a "Asignado" como resultado de la Etapa 5, con la titularidad operativa transferida al técnico de segundo nivel designado. La notificación se enruta automáticamente al técnico responsable, dando inicio al cómputo del tiempo objetivo aplicable conforme al acuerdo de nivel de servicio del caso.

Actor responsable (R). Analista Programador Senior para los casos de prioridad Crítica y Alta. Analista Programador Junior para los casos de prioridad Media y Baja. Para los casos de prioridad Planificada, el técnico designado conforme a la cola de gestión programada del área. El técnico asume la titularidad operativa completa del ticket durante esta etapa.

Actor aprobador (A). Jefe de Proyectos y Desarrollo, quien autoriza los escalamientos hacia el Analista Programador Senior cuando un caso asignado inicialmente a un Junior excede su capacidad técnica, valida el cierre técnico de las incidencias críticas y supervisa el cumplimiento del acuerdo de nivel de servicio dentro de su línea de mando.

Actividades específicas:

- Acceder al ticket en estado "Asignado" a partir de la notificación automática recibida y actualizar el estado a "En atención" como confirmación formal del inicio del trabajo técnico.
- Reproducir o verificar el comportamiento reportado en el sistema afectado, contrastando la descripción del reportante con la evidencia adjunta y, cuando proceda, con el comportamiento observado en el ambiente de pruebas correspondiente.
- Analizar la causa técnica de la incidencia, identificando si corresponde a un error funcional del software, una incidencia de disponibilidad del servicio, una degradación de desempeño o una vulneración de seguridad, conforme al tipo de incidencia previamente clasificado en la Etapa 3.
- Determinar la ruta de resolución aplicable, distinguiendo entre solución directa (ajustes funcionales, reinicio de servicios, restauración de configuraciones), solución mediante despliegue (cambios que requieren paso por el flujo de Gestión de Cambios), o solución temporal mediante alternativa operativa cuando la solución definitiva exceda los tiempos del acuerdo de nivel de servicio.
- Aplicar la solución técnica identificada, documentando en la bitácora del ticket las acciones efectuadas, los componentes intervenidos y las verificaciones de funcionamiento realizadas.
- Verificar que el comportamiento del sistema afectado retorne al estado esperado y que no se hayan generado efectos colaterales sobre otros componentes o módulos.

- Actualizar el estado del ticket a "Resuelto, pendiente de validación del usuario" y notificar al reportante el resultado de la atención, indicando explícitamente las acciones efectuadas y solicitando su validación en la etapa siguiente.

En los casos en los que el técnico identifique, durante el diagnóstico, que la causa técnica excede su capacidad o exige un nivel de especialización mayor al asignado por la regla de enrutamiento, deberá solicitar al Jefe de Proyectos y Desarrollo un escalamiento autorizado hacia el Analista Programador Senior. La solicitud se documenta en la bitácora del ticket con la justificación correspondiente y, una vez autorizada, transfiere la titularidad operativa al técnico de mayor nivel.

Cuando el caso aplique a una situación de reincidencia conforme a los vínculos registrados durante la Etapa 3, el técnico deberá dejar constancia explícita en la bitácora y, al cierre de la etapa, generar la elevación correspondiente hacia la práctica de Gestión de Problemas conforme al lineamiento 5.1.5 de la política institucional.

Entrada. Ticket institucional en estado "Asignado", proveniente de la Etapa 5, con la titularidad operativa transferida al técnico de segundo nivel designado, las dimensiones taxonómicas confirmadas y el acuerdo de nivel de servicio activado con sus tiempos objetivo visibles.

Salida. Ticket institucional actualizado al estado "Resuelto, pendiente de validación del usuario", con la causa técnica identificada y documentada, la solución aplicada con sus acciones y verificaciones registradas en bitácora, el reportante notificado del resultado y, cuando proceda, la elevación a Gestión de Problemas formalmente generada.

Tabla 48. Tiempos, responsables y puntos de control etapa 6.

Tiempo máximo esperado	Responsable operativo	Responsable de aprobación/control	Punto de control automático propuesto en ServiceDesk Plus
Crítica: 7 h Alta: 1.5 días hábiles Media: 4 días hábiles Baja: 7 días hábiles Planificada: programada	Analista Programador Senior (Crítica/Alta) Analista Programador Junior (Media/Baja)	Jefe de Proyectos y Desarrollo, quien autoriza los escalamientos hacia el Analista Programador Senior, valida el cierre técnico de las incidencias críticas y supervisa el cumplimiento del SLA en su línea de mando.	Detectivos: Alertas progresivas de proximidad al vencimiento del SLA en los umbrales del 50%, 75% y 90% del tiempo objetivo, conforme al sistema de semaforización

			institucional descrito en el componente 6.4.3.3. Correctivos automáticos: Generación automática de ticket-problema vinculado ante reincidencia. Preventivos: Bitácora obligatoria de acciones técnicas y verificaciones antes de habilitar el cambio de estado a "Resuelto, pendiente de validación del usuario".
--	--	--	--

Fuente: Elaboración propia.

Campos del ticket actualizados en esta etapa (ManageEngine ServiceDesk Plus):

- Causa técnica identificada (descripción narrativa estructurada).
- Ruta de resolución aplicada: Solución directa, Solución mediante despliegue o Solución temporal mediante alternativa operativa.
- Acciones técnicas efectuadas (detalle por componente intervenido).
- Verificaciones de funcionamiento realizadas y sus resultados.
- Indicador de escalamiento al Analista Programador Senior (cuando aplique).
- Identificador del Jefe de Proyectos y Desarrollo que autorizó el escalamiento (cuando aplique).
- Indicador de elevación a Gestión de Problemas por reincidencia (cuando aplique).
- Identificador del ticket-problema generado en la elevación (cuando aplique).
- Notificación al reportante con resumen de acciones efectuadas.
- Estado del ticket: Resuelto, pendiente de validación del usuario.

Registro de actividades de la etapa (ManageEngine ServiceDesk Plus):

- Identificador del técnico de segundo nivel que ejecutó el diagnóstico y la resolución.
- Fecha y hora de inicio de la atención técnica (*al pasar el estado a "En atención"*).
- Fecha y hora de cierre del diagnóstico y la resolución (al pasar el estado a "Resuelto, pendiente de validación del usuario").

- Bitácora de observaciones técnicas del diagnóstico y la resolución.

Criterio de paso a la siguiente etapa. El ticket se considera apto para avanzar a la Etapa 7 de validación y cierre cuando la causa técnica ha sido identificada y documentada, la solución correspondiente ha sido aplicada con sus acciones y verificaciones registradas, las pruebas de funcionamiento confirman el restablecimiento del comportamiento esperado del sistema, el reportante ha sido notificado del resultado con detalle de las acciones efectuadas, la elevación a Gestión de Problemas ha sido generada cuando el caso lo amerite y el estado del ticket en la plataforma ha sido actualizado a "Resuelto, pendiente de validación del usuario".

Tiempo objetivo asociado. La etapa deberá ejecutarse dentro del tiempo máximo definido por el acuerdo de nivel de servicio aplicable a la prioridad del caso, conforme a la matriz desarrollada en el componente 6.4.3. Esta es la etapa de mayor consumo temporal del flujo, y su cumplimiento es el principal determinante del indicador de tiempo medio de resolución del modelo.

Regla del escalamiento técnico y de la elevación por reincidencia. El modelo contempla dos mecanismos formales de excepción dentro de esta etapa. El primero, el escalamiento técnico, opera cuando el técnico asignado identifica que la causa de la incidencia excede su capacidad y requiere intervención de un perfil de mayor especialización. En tales casos, el técnico solicita el escalamiento al Jefe de Proyectos y Desarrollo, quien autoriza la transferencia de titularidad operativa al Analista Programador Senior. Este mecanismo evita que un ticket permanezca atascado por incapacidad técnica del actor asignado y, al mismo tiempo, asegura que la decisión quede formalmente documentada para fines de aprendizaje organizacional.

El segundo mecanismo, la elevación por reincidencia, opera cuando el técnico identifica que el caso atendido constituye una manifestación adicional de un patrón previamente reportado en el mismo sistema o módulo. En estos casos, la incidencia se resuelve en el ticket en curso, pero adicionalmente se genera un ticket-problema vinculado dentro de la práctica de Gestión de Problemas para el correspondiente análisis de causa raíz. Esta práctica articula la operación inmediata del modelo con la mejora estructural del servicio, conforme al lineamiento de la política

institucional.

Integración con la práctica futura de Gestión de Problemas. El modelo desarrollado en el presente capítulo cubre el ciclo completo de la práctica de Gestión de Incidentes conforme a ITIL 4, pero excluye deliberadamente el diseño completo de la práctica de Gestión de Problemas, conforme a la delimitación de alcance establecido. Sin embargo, la Etapa 6 produce, mediante el mecanismo de elevación por reincidencia, un artefacto institucional que constituye el insumo natural de la práctica de Gestión de Problemas que el banco podría implementar en una fase posterior de madurez del modelo.

Con el propósito de que dicha implementación futura encuentre un punto de entrada estructurado y no requiera rediseñar los mecanismos de elevación ya formalizados, el modelo define desde su versión actual los puntos de integración previstos entre ambas prácticas.

Los puntos de integración previstos se presentan a continuación, ordenados según la dirección del flujo de información entre ambas prácticas.

Código	Punto de integración	Aporte del modelo actual de incidencias	Insumo esperado de la práctica futura
IP-01	Datos del ticket-problema	Identificador del ticket-problema, sistema y módulo afectados, lista de tickets-incidente vinculados, causa técnica preliminar documentada y umbral de la Regla 3 que activó la elevación	Procesamiento del ticket-problema bajo la metodología institucional de análisis de causa raíz que adopte el banco.
IP-02	Estados estandarizados del ticket-problema	Estado inicial "Generado por reincidencia", asignado automáticamente por la plataforma al momento de la elevación	Definición de los estados subsecuentes que rigen el ciclo de vida del ticket-problema (en análisis, causa raíz identificada, solución estructural propuesta, en implementación, cerrado)
IP-03	Catálogo institucional de errores conocidos	El modelo actual no produce errores conocidos; aporta únicamente la materia prima documental contenida en los tickets-incidente vinculados	Construcción y mantenimiento del catálogo institucional de errores conocidos, accesible mediante consulta directa desde la plataforma durante la Etapa 2 de validación y la Etapa 6 de diagnóstico
IP-04	Soluciones temporales centralizadas	La Etapa 6 contempla la ruta "Solución temporal mediante alternativa operativa", pero no centraliza institucionalmente las soluciones temporales aplicadas	Centralización institucional del repositorio de soluciones temporales, disponibles para consulta del segundo nivel técnico desde la plataforma como apoyo a la decisión durante el diagnóstico
IP-05	Retroalimentación hacia el ticket-incidente original	La Regla 3 alimenta el ticket-problema en una sola dirección, sin retorno automático hacia los tickets-incidente que dieron origen a la elevación	Notificación automática de retorno hacia los tickets-incidente vinculados cuando la causa raíz haya sido identificada y la solución estructural haya sido implementada, con cierre

			formal del expediente histórico
IP-06	Indicadores compartidos en el tablero gerencial	Tasa de reincidencia del componente 6.5, junto con el inventario de tickets-problema generados, constituyen los insumos provenientes del modelo de incidencias	Indicadores propios de la práctica futura, tales como tickets-problema abiertos por antigüedad, tiempo medio de identificación de causa raíz y tasa de cierre estructural, reportados al mismo tablero gerencial del componente 6.5

Fuente: Elaboración propia.

Etapa 6 — Diagnóstico y Resolución

Modelo entrada – proceso – salida



Figura 30. Diagrama IPO, etapa 6

Fuentes: Elaboración propia

6.4.2.7.ETAPA 7 - VALIDACIÓN DEL USUARIO Y CIERRE FORMAL

Propósito. Cerrar de manera definitiva el ciclo de vida de la incidencia mediante la certificación formal del reportante de que la solución aplicada resolvió la afectación operativa, y dejar registrada en la plataforma la trazabilidad completa del caso para fines de control, auditoría y mejora continua. La etapa de validación del usuario y cierre formal constituye el handshake institucional entre el área técnica y el área usuaria, y representa el único punto del flujo en el cual el reportante recupera la titularidad operativa del caso para ejercer su rol de certificador. Su finalidad es eliminar la práctica de cierres prematuros sin verificación del usuario identificada durante el diagnóstico, garantizar el cumplimiento del indicador de trazabilidad completa del modelo y asegurar que toda solución aplicada mediante un cambio en el software quede formalmente registrada en el control de cambios institucional.

Actor responsable (R). Colaborador reportante, quien ejecuta la certificación de la

solución aplicada mediante el formato institucional de certificación con sus correspondientes evidencias, sin importar la ruta de resolución registrada en la Etapa 6.

Actor co-responsable. Analista Programador Senior o Analista Programador Junior, según el caso, en su rol de receptor de la certificación del usuario, ejecutor del registro en el control de cambios institucional cuando la ruta de resolución haya correspondido a una solución mediante despliegue, y emisor de la notificación final de cierre con el identificador del control de cambios consignado.

Actor aprobador (A). Jefatura del área de Negocios o de Operaciones del colaborador reportante, según corresponda, quien respalda institucionalmente la certificación efectuada por el reportante conforme al lineamiento aplicable.

Actividades específicas:

- El colaborador reportante recibe la notificación de la plataforma indicando que la solución ha sido aplicada y que el ticket se encuentra pendiente de su certificación formal.
- El colaborador ejecuta las verificaciones funcionales correspondientes en el sistema afectado, confirmando que el comportamiento reportado originalmente ha sido restablecido al estado esperado.
- El colaborador diligencia el formato institucional de certificación con los campos requeridos: descripción del comportamiento previo a la solución, descripción del comportamiento posterior a la solución, pruebas funcionales ejecutadas, resultados obtenidos y declaración formal de conformidad o rechazo.
- El colaborador adjunta las evidencias requeridas por el formato institucional, particularmente las capturas de las pruebas ejecutadas, los resultados observados en el sistema y cualquier validación funcional documentada que respalde su declaración.
- El colaborador carga el formato institucional de certificación con sus evidencias en el ticket dentro del campo institucional dispuesto para ese fin, materializando con ello su visto bueno formal de la solución aplicada.
- El técnico responsable del caso, al recibir la certificación del colaborador en los casos en los cuales la ruta de resolución haya correspondido a una solución mediante despliegue, ejecuta el registro formal del cambio en el control de cambios institucional, consignando

la información requerida por dicho instrumento y vinculándolo al ticket de la incidencia.

- El técnico emite la notificación final al colaborador informando el ingreso formal del cambio en el control de cambios institucional, dejando constancia explícita del identificador asignado por dicho instrumento. Esta actividad aplica únicamente a los casos de solución mediante despliegue.
- El sistema actualiza el estado del ticket a "Cerrado" una vez confirmadas las acciones aplicables según la ruta de resolución, materializando el cierre formal del ciclo de vida de la incidencia.

En los casos en los cuales el colaborador reportante identifique, durante su certificación, que la solución aplicada no resolvió efectivamente la afectación reportada o generó efectos colaterales no aceptables, deberá registrar el rechazo en el formato institucional de certificación con la justificación correspondiente. Ante el rechazo, el ticket retorna al estado "En atención" y la titularidad operativa regresa al técnico de segundo nivel, quien deberá iniciar nuevamente las actividades de diagnóstico y resolución de la Etapa 6 sobre la base de la información adicional aportada por el reportante.

Cuando la ruta de resolución haya correspondido a una solución temporal mediante alternativa operativa, el colaborador diligencia el formato institucional con la modalidad de aceptación parcial, indicando la conformidad con la solución temporal y la dependencia respecto de la solución definitiva futura, la cual se asocia al ticket-cambio o ticket-problema correspondiente.

Entrada. Ticket institucional en estado "Resuelto, pendiente de validación del usuario", proveniente de la Etapa 6, con la causa técnica identificada, la solución aplicada y documentada, las verificaciones técnicas registradas, la ruta de resolución consignada y el reportante notificado del resultado.

Salida. Ticket institucional actualizado al estado "Cerrado", con el formato institucional de certificación diligenciado y adjunto, las evidencias requeridas cargadas, el registro en el control de cambios institucional consignado cuando proceda con su correspondiente identificador, la notificación final al reportante emitida cuando proceda y la trazabilidad completa del ciclo de vida de la incidencia disponible en la plataforma.

Tabla 49. Tiempos, responsables y puntos de control etapa 7.

Tiempo máximo esperado	Responsable operativo	Responsable de aprobación/control	Punto de control automático propuesto en ServiceDesk Plus
Crítica: 1.5 h; Alta: 6 h hábiles; Media: 1.5 días hábiles; Baja: 3 días hábiles; Planificada: 7 días hábiles. Tiempo observable, no evaluable.	Colaborador reportante (certificación); Analista Senior o Junior (registro del control de cambios cuando aplique)	Jefe de Proyectos y Desarrollo, quien autoriza los escalamientos hacia el Analista Programador Senior, valida el cierre técnico de las incidencias críticas y supervisa el cumplimiento del SLA en su línea de mando.	Detectivos: Notificación automática de solicitud de validación al reportante; recordatorios automáticos al usuario por cercanía de vencimiento. Preventivos: Bloqueo de cierre del ticket sin formato institucional de certificación adjunto. Correctivos automáticos: Cierre automático del ticket al recibir certificación positiva; Vinculación automática al control de cambios institucional cuando la solución corresponda a despliegue. De trazabilidad: Registro automático de fecha y hora de cierre.

Fuente: Elaboración propia.

Campos del ticket actualizados en esta etapa (ManageEngine ServiceDesk Plus):

- Formato institucional de certificación diligenciado y sus evidencias.
- Modalidad de certificación: Aceptación, Aceptación parcial por solución temporal o Rechazo.
- Identificador del colaborador reportante que ejecutó la certificación.
- Fecha y hora de la certificación.
- Descripción del comportamiento previo y posterior a la solución consignada por el reportante.
- Pruebas funcionales ejecutadas por el reportante y resultados obtenidos.
- Justificación del rechazo (cuando aplique).
- Identificador del registro en el control de cambios institucional (cuando aplique a

soluciones mediante despliegue).

- Identificador del técnico que ejecutó el registro en el control de cambios (cuando aplique).
- Fecha y hora de ingreso del control de cambios (cuando aplique).
- Notificación final al reportante con identificador del control de cambios (cuando aplique).
- Vínculo con el ticket-cambio o ticket-problema asociado (cuando aplique a soluciones temporales).
- Indicador de trazabilidad completa del ciclo de vida.
- Estado del ticket: Cerrado.

Registro de actividades de la etapa (ManageEngine ServiceDesk Plus):

- Identificador del actor que ejecutó cada acción de la etapa (colaborador para la certificación, técnico para el registro de control de cambios cuando aplique).
- Fecha y hora de cierre de la etapa.
- Bitácora de observaciones de la certificación y del cierre formal.

Criterio de paso al cierre del ciclo. El ticket se considera apto para alcanzar el estado "Cerrado" cuando el colaborador reportante ha diligenciado el formato institucional de certificación con sus evidencias bajo la modalidad correspondiente, el registro en el control de cambios institucional ha sido consignado en los casos de solución mediante despliegue, la notificación final al reportante ha sido emitida cuando proceda y la trazabilidad completa del ciclo de vida ha sido consolidada en la plataforma.

Tiempo objetivo asociado. La certificación deberá ejecutarse dentro del tiempo máximo definido por el acuerdo de nivel de servicio aplicable a la prioridad del caso, conforme a la matriz desarrollada en el componente 6.4.3. Cuando la ruta de resolución haya correspondido a una solución mediante despliegue, el tiempo objetivo incluye la certificación del colaborador, el ingreso del control de cambios y la notificación final al reportante como ventana integral.

Regla de la certificación transversal y de la doble confirmación cruzada en los casos de cambio de software. El modelo adopta la regla de la certificación transversal, conforme a la cual el formato institucional de certificación con sus evidencias se diligencia en todos los casos,

sin importar la ruta de resolución aplicada. Esta regla garantiza que toda incidencia cerrada cuente con un acto formal de conformidad del usuario, materializado en un instrumento institucional verificable, y elimina por completo la práctica de cierres prematuros sin participación del área usuaria identificada durante el diagnóstico.

De manera complementaria, en los casos en los cuales la solución haya implicado un cambio en el software, el modelo exige una doble confirmación cruzada que garantiza la calidad del cierre y la trazabilidad institucional del cambio. La primera confirmación va del colaborador hacia el técnico mediante el diligenciamiento del formato institucional de certificación. La segunda confirmación va del técnico hacia el colaborador mediante la notificación final que informa el ingreso formal del cambio en el control de cambios institucional. Ambas confirmaciones quedan registradas en la plataforma y forman parte del expediente trazable del caso. Esta regla evita que un cambio en producción quede sin certificación funcional del área usuaria y, al mismo tiempo, evita que el colaborador desconozca el ingreso formal del cambio dentro del instrumento de gobierno institucional aplicable.

Regla del rechazo y reapertura. Cuando el colaborador reportante rechaza la certificación porque la solución aplicada no resolvió efectivamente la afectación o generó efectos colaterales no aceptables, el ticket retorna al estado "En atención" y la titularidad operativa regresa al técnico de segundo nivel. La reapertura conserva el identificador único original del ticket para fines de trazabilidad histórica y queda asociada a la información adicional aportada por el reportante en el momento del rechazo, incluida en el formato institucional de certificación. Esta regla evita la práctica de cerrar tickets sobre soluciones aparentes y refuerza la cultura institucional de validación efectiva con el área usuaria.

Encuesta automática de satisfacción posterior al cierre. Como mecanismo complementario al acto formal de certificación descrito previamente, el modelo incorpora una encuesta automática de satisfacción que ManageEngine ServiceDesk Plus envía al colaborador reportante de manera inmediata al cambio del ticket al estado "Cerrado". A diferencia de la certificación formal, que evalúa exclusivamente la eficacia técnica de la solución aplicada, la encuesta evalúa la experiencia integral del usuario durante el ciclo de atención, comprendiendo la oportunidad del primer contacto, la claridad de la comunicación recibida, la percepción sobre el tiempo total de resolución y la satisfacción global con el servicio prestado.

Esta medición adopta la metodología del Customer Satisfaction Score, reconocida por ITIL 4 como instrumento estándar de retroalimentación posterior al cierre (IBM, 2023), y su carácter automático garantiza que el inicio de la retroalimentación no quede sujeto a la disponibilidad voluntaria del colaborador.

Los resultados consolidados alimentan el indicador de satisfacción del tablero gerencial dentro de las medidas de control de la sección 6.5.1., y los casos con calificación por debajo del umbral institucional definido activan revisión obligatoria del Jefe de Proyectos y Desarrollo para identificar causas de insatisfacción y, cuando corresponda, ajustar el proceso o reforzar la capacitación del técnico responsable. El instrumento completo se presenta en el Anexo N de la presente propuesta.

Etapa 7 — Validación del usuario y Cierre formal

Modelo entrada – proceso – salida



Figura 31. Diagrama IPO, etapa 7

Fuente: Elaboración propia.

6.4.3. MATRIZ DE CRITICIDAD, ACUERDOS DE NIVEL DE SERVICIO Y REGLAS DE ESCALAMIENTO

El tercer componente del modelo entrega los tres instrumentos normativos que gobiernan los tiempos del proceso de gestión de incidencias: La matriz de criticidad, la matriz de acuerdos de nivel de servicio y las reglas de escalamiento. Su desarrollo respondió a la necesidad de eliminar la subjetividad operativa identificada durante el diagnóstico, donde la priorización de los casos

dependía del criterio individual del técnico/analista o del Oficial de Soporte y los tiempos de atención no estaban sujetos a un compromiso institucional verificable.

Estos tres instrumentos operan de manera articulada y se vinculan directamente con el flujo de siete etapas desarrollado en el componente [6.4.2](#). La matriz de criticidad alimenta la Etapa 4 al definir cómo se calcula el nivel de prioridad de cada incidencia. La matriz de acuerdos de nivel de servicio gobierna los tiempos objetivo de las etapas del flujo bajo dos categorías diferenciadas: el tiempo administrativo del primer nivel aplicable a las Etapas 1, 2 y 3, y el SLA técnico evaluable aplicable a partir de la Etapa 4. Las reglas de escalamiento, finalmente, operan de manera transversal sobre todas las etapas, activando los mecanismos de respuesta automática cuando el comportamiento del ticket se desvía del esperado por el modelo.

Marco conceptual del componente. El diseño del componente se sustenta en tres referencias del marco teórico del trabajo investigativo. ITIL 4 establece que la priorización de las incidencias debe calcularse mediante el cruce de impacto y urgencia, dado que ambos factores reflejan dimensiones independientes del caso, el impacto mide la magnitud del daño operativo causado, y la urgencia mide la rapidez con la que la solución es requerida (AXELOS, 2019).

COBIT 2019, a través del objetivo de gestión DSS02, exige la formalización de tiempos objetivos verificables como condición para alcanzar niveles superiores de capacidad institucional (ISACA, 2018).

Asimismo, el componente adopta el principio de medir únicamente lo que se puede controlar, aplicado al diseño de los acuerdos de nivel de servicio. Conforme a este principio, los tiempos sujetos a evaluación corresponden exclusivamente a aquellas actividades cuya ejecución depende del área técnica del banco, mientras que las actividades que dependen del usuario reportante o de actos administrativos automáticos se registran como observables sin consecuencia normativa para el área técnica.

6.4.3.1.MATRIZ DE CRITICIDAD

El nivel de prioridad de cada incidencia se calcula mediante el cruce del nivel de impacto operativo y el nivel de urgencia técnica, evaluados durante la Etapa 4 del flujo. Este enfoque permite distinguir con precisión, por ejemplo, una caída total del sistema Inclusión Financiera de una lentitud no transaccional reportada sobre el mismo sistema. Aunque ambos casos comparten el sistema afectado, sus dimensiones de impacto y urgencia son sustancialmente distintas y, en

consecuencia, su nivel de prioridad debe diferir.

Definición de los niveles de impacto operativo. El nivel de impacto operativo evalúa la magnitud del daño causado por la incidencia sobre la operación bancaria. Se determina conforme a tres criterios convergentes: el alcance organizacional de la afectación, el grado de degradación del servicio y la criticidad regulatoria del proceso interrumpido.

Tabla 50. Nivel de impacto operativo.

Nivel de impacto	Descripción institucional
Alto	Afectación que compromete a múltiples unidades organizacionales simultáneamente, interrumpe completamente un servicio bancario o impacta un proceso sujeto a obligaciones regulatorias inmediatas.
Medio	Afectación que compromete a una unidad organizacional o degrada parcialmente un servicio bancario sin interrumpirlo por completo.
Bajo	Afectación que compromete a un usuario individual o a un módulo no transaccional, sin degradación significativa del servicio.

Fuente: Elaboración propia.

Definición de los niveles de urgencia técnica. El nivel de urgencia técnica evalúa la rapidez con la que la solución es requerida para evitar consecuencias mayores. Se determina conforme a tres criterios convergentes: la disponibilidad de soluciones alternativas, la ventana temporal del proceso afectado y la proximidad de obligaciones regulatorias o transaccionales asociadas.

Tabla 51. Niveles de urgencia técnica.

Nivel de urgencia	Descripción institucional
Alta	No existen soluciones alternativas operativas, la ventana temporal del proceso afectado es inmediata o existen obligaciones regulatorias o transaccionales próximas a su vencimiento.
Media	Existen soluciones alternativas operativas limitadas, la ventana temporal del proceso afectado permite tolerancia parcial o las obligaciones asociadas no son inminentes.
Baja	Existen soluciones alternativas operativas plenamente funcionales, la ventana temporal del proceso afectado es amplia y no existen obligaciones inminentes asociadas.

Fuente: Elaboración propia.

Matriz de cruce impacto × urgencia. El nivel de prioridad resultante se determina mediante el cruce de las dos dimensiones anteriores, conforme a la siguiente matriz:

Tabla 52. Matriz de impacto x urgencia.

	Urgencia Alta	Urgencia Media	Urgencia Baja
Impacto Alto	Crítica	Alta	Media
Impacto Medio	Alta	Media	Baja

	Urgencia Alta	Urgencia Media	Urgencia Baja
Impacto Bajo	Media	Baja	Planificada

Fuente: Elaboración propia.

El nivel Crítica se reserva para los casos de máximo impacto y máxima urgencia simultáneos, situación que activa los tiempos de SLA más estrictos del modelo y permite la activación de la guardia técnica fuera de horario hábil cuando así corresponda. El nivel Planificada se aplica a los casos de menor impacto y menor urgencia, los cuales se incorporan al cronograma de gestión programada del área en lugar de ser atendidos bajo el SLA general.

Sistema afectado como agravante. El nivel de prioridad calculado por el cruce impacto $\times$ urgencia puede ser elevado automáticamente cuando el sistema afectado pertenece al catálogo institucional de sistemas críticos del banco. Este catálogo se construye progresivamente conforme a la evidencia operativa y no requiere un inventario exhaustivo de todos los sistemas del banco como precondition para la implementación del modelo.

Como punto de partida, el catálogo se inicia con los cuatro sistemas identificados durante el diagnóstico del presente trabajo investigativo, los cuales registraron los mayores índices de recurrencia de fallas durante el período analizado:

Tabla 53. Sistemas reincidentes.

Sistema crítico inicial	Origen del reconocimiento
Inclusión Financiera	Recurrencia identificada en el Capítulo IV
ENEE	Recurrencia identificada en el Capítulo IV
RAP	Recurrencia identificada en el Capítulo IV
Conciliación SINAP	Recurrencia identificada en el Capítulo IV

Fuente: Elaboración propia.

Cuando un ticket de cualquiera de estos cuatro sistemas reciba una prioridad calculada Media, Baja o Planificada, el motor de la plataforma incrementará automáticamente un nivel la prioridad asignada, conforme a la siguiente lógica: Planificada se eleva a Baja, Baja se eleva a Media y Media se eleva a Alta. La regla no opera sobre prioridades calculadas Crítica o Alta, dado que el modelo no contempla niveles superiores a Crítica.

Los demás sistemas del banco se tratan bajo la categoría "Otro sistema" dentro del modelo, operando con la regla general de cruce impacto $\times$ urgencia sin agravamiento automático. La Gerencia de Tecnología y Comunicaciones puede incorporar nuevos sistemas al catálogo crítico mediante acto administrativo formal, fundamentado en evidencia operativa observada durante la

operación del modelo o en cambios regulatorios o estratégicos que lo justifiquen.

6.4.3.2.MATRIZ DE ACUERDOS DE NIVEL DE SERVICIO

Los tiempos objetivo del modelo se organizan en dos grandes categorías. La primera comprende los tiempos evaluables, sujetos a medición formal y consecuencia normativa para el área técnica, e incluye el tiempo administrativo del primer nivel aplicable a las Etapas 1 a 3 y el SLA técnico aplicable a las Etapas 4 a 6. La segunda comprende los tiempos observables, registrados con fines estadísticos pero sin consecuencia normativa, e incluye la validación del usuario y el cierre formal correspondientes a la Etapa 7. Esta diferenciación responde al principio de medir únicamente lo que se puede controlar, conforme al cual los tiempos cuya ejecución depende del colaborador reportante o de actos administrativos automáticos quedan fuera del esquema de evaluación del área técnica.

Tabla 54. Matriz SLA

Etapas	Crítica	Alta	Media	Baja	Planificada
Etapas 1 - Registro	10 min hábiles	10 min hábiles	10 min hábiles	10 min hábiles	10 min hábiles
Etapas 2 - Validación	30 min hábiles	30 min hábiles	30 min hábiles	30 min hábiles	30 min hábiles
Etapas 3 - Clasificación	20 min hábiles	20 min hábiles	20 min hábiles	20 min hábiles	20 min hábiles
Etapas 4 - Priorización	15 min	1 h hábil	2 h hábiles	4 h hábiles	Programada
Etapas 5 - Asignación	15 min	1 h hábil	2 h hábiles	4 h hábiles	Programada
Etapas 6 - Diagnóstico y Resolución	7 h	1.5 días hábiles	4 días hábiles	7 días hábiles	Programada
Etapas 7 - Validación del usuario y Cierre formal	1.5 h	6 h hábiles	1.5 días hábiles	3 días hábiles	7 días hábiles
Tiempo administrativo del primer nivel (Etapas 1 a 3)	1 hora hábil	1 hora hábil	1 hora hábil	1 hora hábil	1 hora hábil
SLA técnico evaluable (Etapas 4 a 6)	7.5 horas	2 días hábiles	4.5 días hábiles	8 días hábiles	Conforme a cronograma

Fuente: Elaboración propia.

Tiempo administrativo del primer nivel. Aplicable de manera uniforme a todo ticket, independientemente del nivel de prioridad que se calcule posteriormente en la Etapa 4.

SLA técnico evaluable. Aplicable a partir de la Etapa 4, diferenciado por nivel de prioridad y por momento del ciclo. El día hábil se asume de ocho horas conforme a la jornada laboral institucional.

Tiempos observables no evaluables. Tiempos registrados con fines estadísticos pero excluidos del esquema de evaluación formal del área técnica.

La validación del usuario depende del colaborador reportante y queda fuera del SLA evaluable. El cierre formal se ejecuta de manera automática por la plataforma al recibir la certificación del usuario, sin intervención humana que pueda retrasarlo.

6.4.3.3.REGLAS DE ESCALAMIENTO

El modelo contempla tres tipos de reglas de escalamiento que operan de manera transversal sobre el flujo de siete etapas. Cada regla responde a un tipo distinto de desviación respecto del comportamiento esperado del ticket y activa una respuesta automática de la plataforma o de los actores institucionales designados.

Regla 1 - Escalamiento por SLA. Esta regla opera durante toda la ventana del SLA técnico evaluable y activa alertas y reasignaciones automáticas cuando los tiempos objetivo se aproximan al vencimiento o lo rebasan. Sus umbrales y acciones son los siguientes:

Tabla 55. Reglas de escalamiento.

Umbral	Trigger	Acción automática
50% del SLA del momento del ciclo	Notificación informativa al técnico responsable	Alerta de avance en la plataforma
75% del SLA del momento del ciclo	Notificación de alerta al técnico responsable y al Jefe de Proyectos y Desarrollo	Alerta amarilla en la plataforma
90% del SLA del momento del ciclo	Notificación crítica anticipada al técnico responsable, al Jefe de Proyectos y Desarrollo y al Gerente de Tecnología y Comunicaciones	Alerta naranja en la plataforma como aviso de inminente vencimiento
100% del SLA del momento del ciclo	Vencimiento del SLA y notificación obligatoria al Jefe de Proyectos y Desarrollo	Alerta roja en la plataforma y registro como SLA incumplido
100% del SLA con prioridad Crítica	Vencimiento del SLA crítico	Convocatoria automática a sesión de emergencia con el Jefe de Proyectos y Desarrollo, Analista Programador Senior y técnico responsable

Fuente: Elaboración propia.

Adicionalmente, la regla contempla la reasignación automática por saturación. La reasignación automática por saturación operativa se desarrolla en el componente [6.4.2.5](#) bajo el mecanismo MR-02, los nuevos tickets de prioridad Crítica o Alta se enrutan automáticamente al

Analista Programador Senior, sin perjuicio de la regla general de enrutamiento descrita en la Etapa 5.

Regla 2 - Reclasificación durante la atención. Esta regla opera cuando el técnico responsable identifica, durante el diagnóstico o la resolución, que el nivel de prioridad asignado originalmente no corresponde a la dimensión real del caso, sea porque el impacto resultó mayor al evaluado inicialmente o porque la urgencia se modificó por circunstancias técnicas descubiertas durante la atención.

Tabla 56. Reclasificación de incidencias.

Condición	Procedimiento	Tratamiento del SLA
El técnico identifica que la prioridad debe elevarse	Solicita reclasificación al Jefe de Proyectos y Desarrollo, justificada por escrito en la bitácora del ticket	El SLA se recalcula desde el momento de la reclasificación, conservando registro del tiempo consumido bajo la prioridad anterior
El técnico identifica que la prioridad debe reducirse	Solicita reclasificación al Jefe de Proyectos y Desarrollo, justificada por escrito en la bitácora del ticket	El SLA se mantiene conforme a la prioridad original como compromiso ya adquirido con el usuario
Concurrencia de varias reclasificaciones sobre un mismo ticket	Procede como excepción que requiere autorización adicional de la Gerencia de Tecnología y Comunicaciones	Tratamiento caso por caso

Fuente: Elaboración propia.

Toda reclasificación debe quedar formalmente documentada en la bitácora del ticket y queda sujeta a la supervisión de consistencia que el Jefe de Proyectos y Desarrollo ejerce sobre la calidad de la priorización institucional. La regla evita que los técnicos atiendan casos bajo los tiempos correspondientes a una prioridad menor cuando la realidad operativa demanda un tratamiento más estricto.

Regla 3 - Vinculación con Gestión de Problemas por reincidencia. Esta regla operacionaliza el lineamiento de la política institucional y opera cuando el técnico responsable identifica que el caso atendido constituye una manifestación adicional de un patrón previamente reportado en el mismo sistema o módulo. Los umbrales que activan la elevación a la práctica de Gestión de Problemas son los siguientes:

Tabla 57. Gestión de problemas por reincidencia.

Condición de reincidencia	Acción automática
Tres tickets cerrados sobre el mismo sistema y módulo con causa técnica equivalente en una ventana de treinta días	Generación automática de ticket-problema vinculado, asignado al Analista Programador Senior para análisis de causa raíz
Dos tickets cerrados sobre un sistema clasificado como crítico (Inclusión Financiera, ENEE, RAP, Conciliación SINAP) con causa técnica equivalente en una ventana de quince días	Generación automática de ticket-problema vinculado, asignado al Analista Programador Senior para análisis de causa raíz
Cualquier ticket sobre el cual el técnico identifique relación causal con un patrón observable previo, sin alcanzar los umbrales anteriores	Generación manual de ticket-problema vinculado por iniciativa del técnico, con justificación en la bitácora

Fuente: Elaboración propia.

La regla transforma el modelo de uno meramente reactivo a uno que aprende de los patrones observados. Su aplicación es la principal vía mediante la cual el modelo aborda la causa estructural de la tasa de reincidencia identificada durante el diagnóstico, dado que el análisis individual de cada caso por separado nunca habría revelado la naturaleza recurrente de las fallas.

Sistema institucional de semaforización del cumplimiento del SLA. Los umbrales declarados en la [Tabla 52](#) operan en la lógica interna del motor de escalamiento, pero su consumo por parte de los actores institucionales requiere una representación visual unificada que permita identificar de manera inmediata el estado de cumplimiento del SLA de cada ticket activo. Con ese propósito, el modelo formaliza un sistema institucional de semaforización que consolida en cinco colores el estado de avance respecto del tiempo objetivo y articula la notificación escalonada a los actores responsables. La semaforización opera de manera automática en ManageEngine ServiceDesk Plus.

Semaforización de alertas de SLA

Color	Umbral de activación	Significado institucional	Acción automática en la plataforma	Destinatarios de la notificación
Verde	Del inicio al 50% del SLA del momento del ciclo	Cumplimiento dentro del margen esperado, sin riesgo identificado	Registro de avance en la plataforma, sin notificación adicional	Técnico responsable del ticket
Amarillo	Más de 50% y hasta el 75% del SLA del momento del ciclo	Cumplimiento bajo observación, requiere seguimiento del responsable jerárquico	Alerta amarilla en la plataforma y notificación de seguimiento	Técnico responsable y Jefe de Proyectos y Desarrollo
Naranja	Más del 75% y hasta el 90% del SLA del momento del ciclo	Cumplimiento en riesgo de vencimiento, exige acción correctiva inmediata	Alerta naranja en la plataforma y notificación crítica anticipada	Técnico responsable, Jefe de Proyectos y Desarrollo y Gerente de Tecnología y Comunicaciones
Rojo	Vencimiento del SLA al 100% del tiempo objetivo	Incumplimiento consumado, registrado formalmente como SLA fallido	Alerta roja en la plataforma, registro como SLA incumplido y, en casos de prioridad Crítica, convocatoria automática a sesión de emergencia	Técnico responsable, Jefe de Proyectos y Desarrollo y Gerente de Tecnología y Comunicaciones
Negro	Vencimiento del SLA con concurrencia de afectación regulatoria, afectación a la continuidad operativa o afectación a un sistema clasificado como crítico	Incumplimiento institucionalmente reportable, requiere activación de los actores de continuidad y cumplimiento del banco	Alerta negra en la plataforma, escalamiento institucional automático y registro como evento institucional reportable	Anteriores más Coordinador de Continuidad del Negocio y Riesgo Tecnológico, Jefe de Riesgo Operativo y Cumplimiento Regulatorio, y Jefe de Auditoría de TI.

Figura 32. Sistema institucional de semaforización del cumplimiento del SLA.

Fuente: Elaboración propia.

6.4.3.4.MATRIZ RA DEL PROCESO DE GESTIÓN DE INCIDENCIAS DE SOFTWARE

El modelo adopta la modalidad **RA simplificada**, en lugar de la versión clásica RACI completa. Esta decisión responde a tres consideraciones prácticas. En primer lugar, la estructura de la Gerencia de Tecnología y Comunicaciones es relativamente compacta, lo cual reduce la utilidad operativa de niveles adicionales de consulta e información que suelen caracterizar a las organizaciones más grandes. En segundo lugar, la simplicidad del esquema facilita su comunicación, comprensión y adopción por parte de los actores involucrados durante la implementación. En tercer lugar, el esquema RA cubre la responsabilidad sustantiva del proceso, que es lo que ITIL 4 considera condición mínima para que una práctica alcance el estado documentado y formalizado (AXELOS, 2019).

La convención utilizada por la matriz es la siguiente. La letra **R** designa al rol **Responsable**, es decir, el actor encargado de ejecutar directamente la actividad de la etapa correspondiente. La letra **A** designa al rol **Accountable**, es decir, el actor que rinde cuentas por el resultado de la etapa, valida su cumplimiento y asume la responsabilidad institucional final.

Cuando un rol comparte ejecución bajo condiciones diferenciadas, se indica mediante notas al pie de la matriz.

Roles considerados en la matriz. La matriz considera siete roles institucionales que corresponden a la estructura organizacional vigente de la Gerencia de Tecnología y Comunicaciones, conforme al organigrama del banco:

Tabla 58. Roles en la matriz RA.

#	Rol	Descripción de su participación principal
1	Colaborador reportante de Negocios u Operaciones	Reporta directamente las incidencias detectadas durante su operación y certifica las soluciones aplicadas.
2	Oficial de Soporte Proyectos / Help Desk	Ejerce la función de Mesa de Servicio como primer nivel de atención para los casos generales.
3	Oficial de Soporte Cash Management	Ejerce la función de Mesa de Servicio como primer nivel de atención para los casos del sistema Cash Management.
4	Analista Programador Senior	Atiende los casos de prioridad Crítica y Alta como segundo nivel técnico.
5	Analistas Programadores Junior	Atienden los casos de prioridad Media y Baja como segundo nivel técnico.
6	Jefe de Proyectos y Desarrollo	Coordina tácticamente la operación del modelo y ejerce la rendición de cuentas sobre las etapas del flujo.
7	Gerente de Tecnología y Comunicaciones	Ejerce la autoridad estratégica del modelo, aprueba la política y autoriza excepciones formales.

Fuente: Elaboración propia.

Actores institucionales internos activados por escalamiento. La matriz RA del proceso considera los siete roles operativos de la Gerencia de Tecnología y Comunicaciones que ejecutan o rinden cuentas sobre las etapas del flujo. Sin embargo, el modelo reconoce que ciertas incidencias, particularmente aquellas que alcanzan el nivel Negro del sistema institucional de semaforización descrito en el componente 6.4.3.3, generan obligaciones institucionales que trascienden el ámbito técnico y requieren la activación formal de actores internos del banco con competencias específicas en continuidad operativa, riesgo operativo y auditoría de tecnología. Estos actores no participan en la ejecución ordinaria del flujo de gestión de incidencias y, por esa razón, no figuran en la matriz RA principal. Su rol institucional es exclusivamente de recepción de notificación obligatoria, escalamiento de decisión cuando corresponda dentro de sus competencias, y eventual incorporación al expediente del caso para fines de auditoría posterior.

Tabla 59. Actores institucionales internos activados por escalamiento.

Actor institucional	Adscripción organizacional	Condición de activación	Naturaleza de la participación
Coordinador de Continuidad del Negocio y Riesgo Tecnológico	Gerencia de Riesgos	Vencimiento del SLA en sistema crítico con afectación a la continuidad operativa, o incidencia que active formalmente el plan institucional de continuidad del negocio	Notificación obligatoria y coordinación con el equipo técnico para evaluar la activación de procedimientos de continuidad
Jefe de Riesgo Operativo y Cumplimiento Regulatorio	Gerencia de Riesgos	Vencimiento del SLA con afectación a procesos sujetos a obligaciones regulatorias internas, o incidencia que comprometa el cumplimiento de plazos regulatorios documentados	Notificación obligatoria y evaluación del impacto regulatorio interno con elevación a la Gerencia cuando corresponda
Jefe de Auditoría de TI	Auditoría Interna	Vencimiento del SLA con afectación a la integridad de información, a controles de tecnología o a evidencia documental requerida por auditoría	Notificación obligatoria y eventual incorporación del expediente del ticket al registro de eventos de auditoría

Fuente: Elaboración propia con base en la estructura organizacional vigente de Banco FICENSA

Tabla 60. Matriz RA del proceso.

Etapas del proceso	Colaborador	Oficial HD	Oficial CM	Analista Sr	Analista Jr	Jefe PyD	Gerente TIC
Etapas 1 - Registro	R ¹	R ²	R ²	—	—	A	—
Etapas 2 - Validación	—	R ³	R ³	—	—	A	—
Etapas 3 - Clasificación	—	R ³	R ³	—	—	A	—
Etapas 4 - Priorización	—	R ³	R ³	—	—	A	—
Etapas 5 - Asignación	—	R ³	R ³	—	—	A	—

¹ El colaborador reportante es responsable principal del registro directo en el portal de autoservicio de ManageEngine ServiceDesk Plus.

² El Oficial de Soporte Proyectos / Help Desk o el Oficial de Soporte Cash Management (según el sistema afectado) asume el registro asistido únicamente bajo imposibilidad técnica documentada del colaborador, conforme al lineamiento 5.1.2 de la política institucional.

³ El Oficial de Soporte Proyectos / Help Desk atiende los casos generales. El Oficial de Soporte Cash Management atiende exclusivamente los casos del sistema Cash Management.

Etapas del proceso	Colaborador	Oficial HD	Oficial CM	Analista Sr	Analista Jr	Jefe PyD	Gerente TIC
Etapas 6 - Diagnóstico y Resolución	—	—	—	R ⁴	R ⁵	A	—
Etapas 7 - Validación del usuario y Cierre formal	R ⁶	—	—	R ⁷	R ⁷	A	—

Fuente: Elaboración propia.

6.4.4. MAPA DE POLÍTICAS Y PROCESOS INSTITUCIONALES

El diseño del modelo no se agota en la formulación de una política y un flujo de trabajo nuevos, sino que exige determinar con precisión qué componentes del marco normativo y procedimental vigente de Banco FICENSA deben crearse, actualizarse o complementarse para que la propuesta resulte aplicable. Con este propósito se construye el presente mapa, cuyo criterio metodológico consiste en derivar cada acción normativa directamente de una conclusión del estudio, garantizando la trazabilidad entre el diagnóstico, la propuesta y la gestión del cambio institucional. De esta forma, los hallazgos dejan de ser enunciados analíticos para convertirse en intervenciones documentales verificables.

Cada fila del mapa tipifica la acción requerida en tres categorías: *Crear*, cuando el instrumento no existe en el banco; *Actualizar*, cuando existe un documento vigente que debe modificarse para incorporar la gestión de incidencias de software; y *Complementar*, cuando el instrumento vigente conserva su validez, pero requiere disposiciones adicionales. Las acciones aquí consignadas constituyen intervenciones propuestas y no cambios ya ejecutados, por lo que sus efectos deben interpretarse como beneficios esperados sujetos a implementación y verificación posterior.

⁴ El Analista Programador Senior es responsable de los casos de prioridad Crítica y Alta, conforme a la regla institucional de enrutamiento descrita en la Etapa 5 del flujo.

⁵ Los Analistas Programador Junior son responsables de los casos de prioridad Media y Baja, distribuidos por disponibilidad operativa, conforme a la regla institucional de enrutamiento descrita en la Etapa 5.

⁶ El colaborador reportante es responsable principal de la certificación funcional de la solución, mediante el formato institucional de certificación con sus evidencias.

⁷ El Analista Programador Senior o Junior (según el que haya atendido el caso) es responsable del registro en el control de cambios institucional y de la notificación final al reportante, únicamente cuando la solución haya implicado un cambio de software.

Tabla 61. Mapa de políticas y procesos institucionales a actualizar según las conclusiones del estudio.

Conclusión	Documento o proceso institucional impactado	Estado actual	Acción requerida	Descripción del cambio	Horizonte
Conclusión 1	Política Institucional de Gestión de Incidencias de Software.	Inexistente.	Crear	Oficializar el marco normativo único que formaliza el modelo basado en ITIL 4, en respuesta a la operación parcialmente informal y dispersa ubicada en el nivel 1 de capacidad, con el fin de fortalecer la trazabilidad, la medición y el control operativo de las incidencias.	Inmediato
Conclusión 2	Procedimiento operativo de la Mesa de Servicio institucional.	Vigente para otras solicitudes de TI, sin cobertura de las incidencias de software.	Actualizar	Ampliar el alcance de la Mesa de Servicio existente para incorporar las incidencias de software bajo un criterio uniforme de registro y seguimiento, atendiendo la dispersión de medios y la falta de historial completo de los casos.	6 meses
Conclusión 3	Matriz de Acuerdos de Nivel de Servicio y reglas de escalamiento.	Inexistente.	Crear	Formalizar tiempos objetivo de atención y resolución diferenciados por nivel de criticidad, con reglas claras de escalamiento, atendiendo la amplia diferencia entre la primera respuesta y la resolución definitiva.	Inmediato
Conclusión 4	Rutina de seguimiento priorizado por sistema y área en la Mesa de Servicio.	Inexistente.	Crear	Establecer revisiones periódicas de recurrencia enfocadas en el área de Operaciones, las fallas funcionales y el sistema Inclusión Financiera, sin descuidar el resto de los sistemas que soportan la operación diaria.	6 meses
Conclusión 5	Políticas de Seguridad de la Información.	Vigente.	Actualizar	Incorporar el registro obligatorio con campos mínimos estandarizados, la trazabilidad íntegra del ciclo de vida y la	6 meses

Conclusión	Documento o proceso institucional impactado	Estado actual	Acción requerida	Descripción del cambio	Horizonte
				conservación de evidencia de las incidencias de software, atendiendo la pérdida de evidencia asociada al 62.5% de informalidad.	
Conclusión 6	Matriz de Indicadores Clave de Desempeño (KPIs).	Definida en el estudio, sin institucionalizar.	Crear	Formalizar la matriz de KPIs como instrumento institucional de revisión periódica y complementarla con métricas de cumplimiento de SLA una vez incorporado el flujo formal, partiendo de la línea base establecida.	6 meses
Conclusión 7	Catálogo de servicios y categorías, y configuración del flujo en ManageEngine ServiceDesk Plus.	Vigente para otras solicitudes de TI, sin parametrización del flujo de incidencias de software.	Complementar	Parametrizar el flujo formal de siete etapas y la taxonomía de clasificación en la plataforma existente, sin adquirir una herramienta nueva, para reducir la brecha del nivel 1 al nivel 3 (Establecido).	6 meses

Fuente: Elaboración propia

El mapa evidencia que la aplicabilidad del modelo no depende únicamente de la creación de instrumentos nuevos, sino de una intervención articulada sobre tres frentes complementarios. El primero corresponde a la creación de los componentes nucleares que el banco no posee, como la política institucional, la matriz de acuerdos de nivel de servicio, la matriz de indicadores y, en una fase posterior, la práctica de Gestión de Problemas.

El segundo corresponde a la actualización de la normativa vigente que resulta directamente afectada, particularmente las Políticas de Seguridad de la Información y el procedimiento operativo de la Mesa de Servicio.

El tercero corresponde a la complementación de la plataforma ManageEngine ServiceDesk Plus mediante la parametrización del flujo y la taxonomía institucional. Esta distribución permite aprovechar la infraestructura y la normativa existentes, evita la duplicación del marco documental del banco y concentra el esfuerzo institucional en las intervenciones

estrictamente derivadas de la evidencia.

En conjunto, el mapa traduce las conclusiones del estudio en una ruta de actualización normativa y procedimental verificable, de modo que los hallazgos del diagnóstico no permanezcan como enunciados analíticos, sino que se materialicen en acciones concretas cuya ejecución y efectos deberán confirmarse durante la implementación del modelo.

6.5.MEDIDAS DE CONTROL

El presente apartado consolida los indicadores y mecanismos que permitirán a la Gerencia de Tecnología y Comunicaciones medir la eficacia y eficiencia del modelo propuesto. Las medidas se organizan en cuatro bloques: el tablero maestro de indicadores, el ciclo de control, las acciones ante desviación y los roles de supervisión.

6.5.1. TABLEROS DE KPIS

Con el propósito de fortalecer el seguimiento operativo del modelo, los tableros de KPIs incorporan no solo la medición periódica de los indicadores, sino también la periodicidad formal de revisión y los responsables encargados de validar sus resultados. Esta definición permite que cada indicador cuente con una ruta clara de supervisión, evitando que la medición quede limitada a la generación automática de reportes.

KPIs del modelo con periodicidad de revisión y responsables



Indicador	Descripción	Frecuencia de medición	Herramienta	Límite mínimo aceptable	Límite máximo aceptable	Periodicidad de revisión	Responsable de revisión
Porcentaje de incidencias con registro formal	Proporción de incidencias gestionadas mediante ticket en SDP sobre el total reportado.	Mensual	ManageEngine ServiceDesk Plus	95%	100%	Mensual	Jefe de Proyectos y Desarrollo
Cumplimiento del tiempo administrativo del primer nivel	Proporción de tickets que cumplen los tiempos uniformes de las Etapas 1 a 3.	Mensual	ManageEngine ServiceDesk Plus	90%	100%	Mensual	Jefe de Proyectos y Desarrollo
Cumplimiento del SLA técnico evaluable	Proporción de tickets que cumplen el SLA técnico aplicable a las Etapas 4 a 6.	Mensual	ManageEngine ServiceDesk Plus	85%	100%	Mensual, con revisión gerencial trimestral	Jefe de Proyectos y Desarrollo; Gerente de Tecnología y Comunicaciones en revisión trimestral
Tiempo medio de resolución (MTTR)	Tiempo promedio desde el registro hasta la resolución técnica.	Mensual	ManageEngine ServiceDesk Plus	0	Conforme al SLA por prioridad	Mensual	Jefe de Proyectos y Desarrollo, con apoyo del Analista Programador Senior
Tasa de reincidencia	Proporción de incidencias reincidentes sobre el total cerrado en la ventana definida.	Trimestral	ManageEngine ServiceDesk Plus	0%	20%	Trimestral	Analista Programador Senior y Jefe de Proyectos y Desarrollo
Porcentaje de trazabilidad completa del ciclo	Proporción de tickets cerrados con ciclo de vida íntegramente documentado.	Trimestral	Auditoría interna sobre SDP	90%	100%	Trimestral	Auditoría Interna y Jefe de Proyectos y Desarrollo
Nivel de satisfacción del usuario	Calificación promedio del reportante tras el cierre del ticket.	Trimestral	Encuesta automática en SDP	4.0 de 5.0	5.0 de 5.0	Trimestral	Jefe de Proyectos y Desarrollo

Figura 33. KPIs del modelo.

Fuente: Elaboración propia.

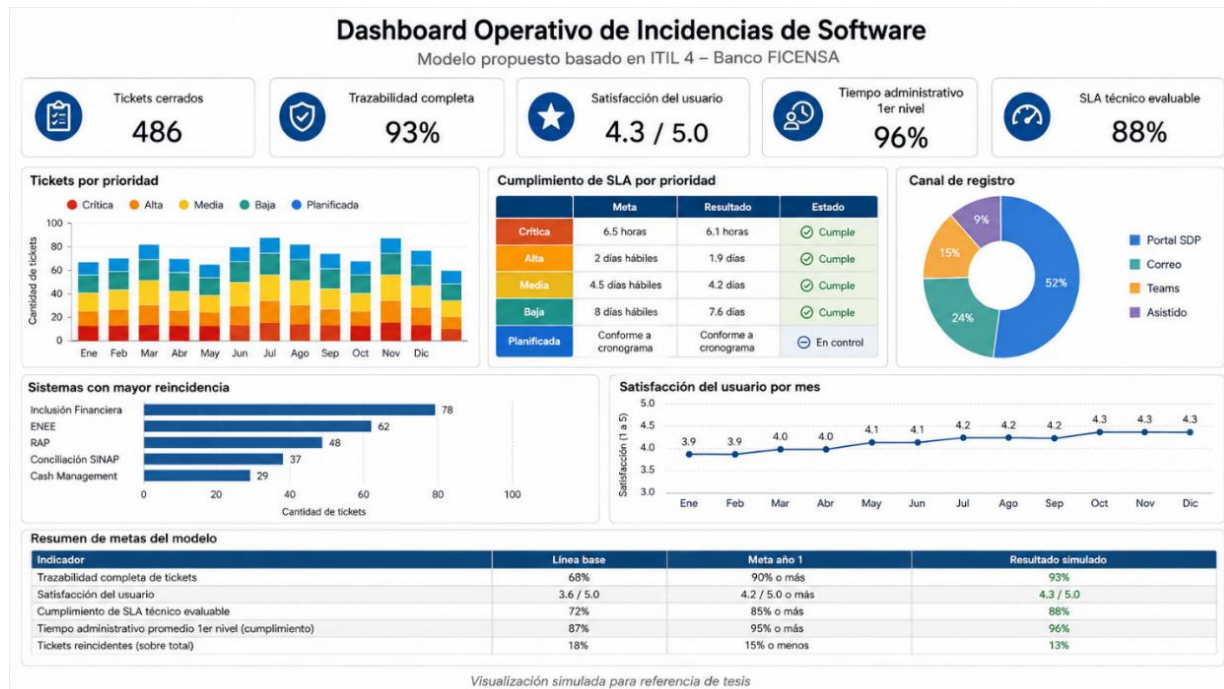


Figura 34. Borrador de tablero de KPI (Versión 1).

Fuente: Elaboración propia.

Nota: La figura corresponde a una visualización simulada para fines de diseño de la propuesta, no sustituye los resultados históricos del diagnóstico documental.

La figura presenta una visualización operativa simulada del modelo propuesto para el seguimiento de incidencias de software en Banco FICENSA. El tablero integra indicadores de control como tickets cerrados, trazabilidad completa, satisfacción del usuario, cumplimiento del tiempo administrativo y cumplimiento del SLA técnico evaluable. Asimismo, incorpora vistas complementarias sobre prioridades, canales de registro, sistemas con mayor reincidencia, satisfacción mensual y resumen de metas del modelo, permitiendo una lectura consolidada del desempeño operativo del proceso.

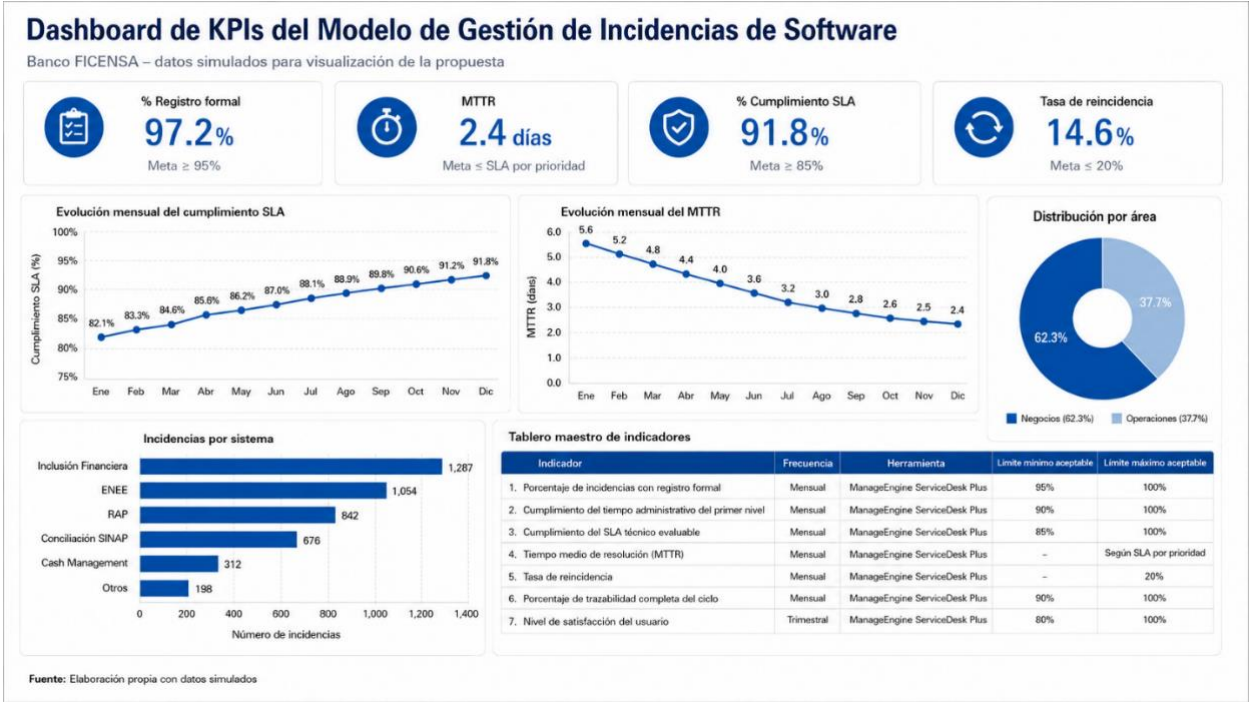


Figura 35. Borrador de tablero de KPI (Versión 2)

Fuente: Elaboración propia.

Nota: La figura corresponde a una visualización simulada del tablero de indicadores propuesto, su finalidad es representar la organización esperada de los KPIs una vez configurado el mecanismo de seguimiento institucional.

La figura muestra un tablero simulado de KPIs orientado al seguimiento táctico del modelo de gestión de incidencias de software. Su propósito es visualizar el comportamiento de

indicadores clave como porcentaje de registro formal, MTTR, cumplimiento de SLA y tasa de reincidencia, junto con tendencias mensuales, distribución por área, incidencias por sistema y tablero maestro de indicadores. Esta representación permite evidenciar cómo los datos generados por ServiceDesk Plus pueden convertirse en insumos para la revisión periódica, toma de decisiones y mejora continua del proceso.

6.5.2. CICLO DE CONTROL

El ciclo de control del modelo opera de manera continua y se sustenta en la práctica de mejora continua definida por ITIL 4 como una de sus prácticas generales de gestión, así como en el *Continual Improvement Model* descrito por (AXELOS, 2019). Este modelo, integrante del Sistema de Valor del Servicio, organiza la mejora en siete pasos iterativos: definición de la visión, evaluación del estado actual, formulación del estado objetivo, determinación de las acciones requeridas, ejecución de la acción, verificación del resultado y mantenimiento del impulso de mejora.

Con el propósito de adaptar el modelo de mejora continua de ITIL 4 a la realidad operativa de Banco FICENSA, el ciclo de control articula los siete pasos del marco en tres fases consolidadas, sin alterar su lógica iterativa ni su orientación hacia la co-creación de valor.

Fase 1. Medición y diagnóstico: Comprende la recolección sistemática de los indicadores, su comparación contra los límites aceptables establecidos y la identificación de desviaciones respecto al desempeño esperado del modelo. Esta fase materializa los pasos 1, 2 y 3 del modelo de ITIL 4 (visión, estado actual y estado objetivo), dado que los KPIs operan simultáneamente como referencia de lo deseado, retrato del estado presente y herramienta para detectar la brecha entre ambos.

Fase 2. Análisis y planificación. Comprende el análisis de la causa raíz de las desviaciones detectadas, la formulación del plan de acción correctivo correspondiente, la designación de responsables y la fijación de plazos verificables.

Fase 3. Ejecución, verificación y consolidación. Comprende la implementación del plan de acción, la Re verificación de los indicadores en el ciclo de medición siguiente y la institucionalización de las mejoras que hayan demostrado eficacia mediante su incorporación al diseño del proceso, a la configuración de ManageEngine ServiceDesk Plus o a la política

institucional aprobada. Esta fase materializa los pasos 5, 6 y 7 del modelo de ITIL 4 (ejecución, verificación del resultado y mantenimiento del impulso de mejora), y garantiza que los aprendizajes operativos del ciclo se conviertan en cambios estructurales y no en correcciones aisladas

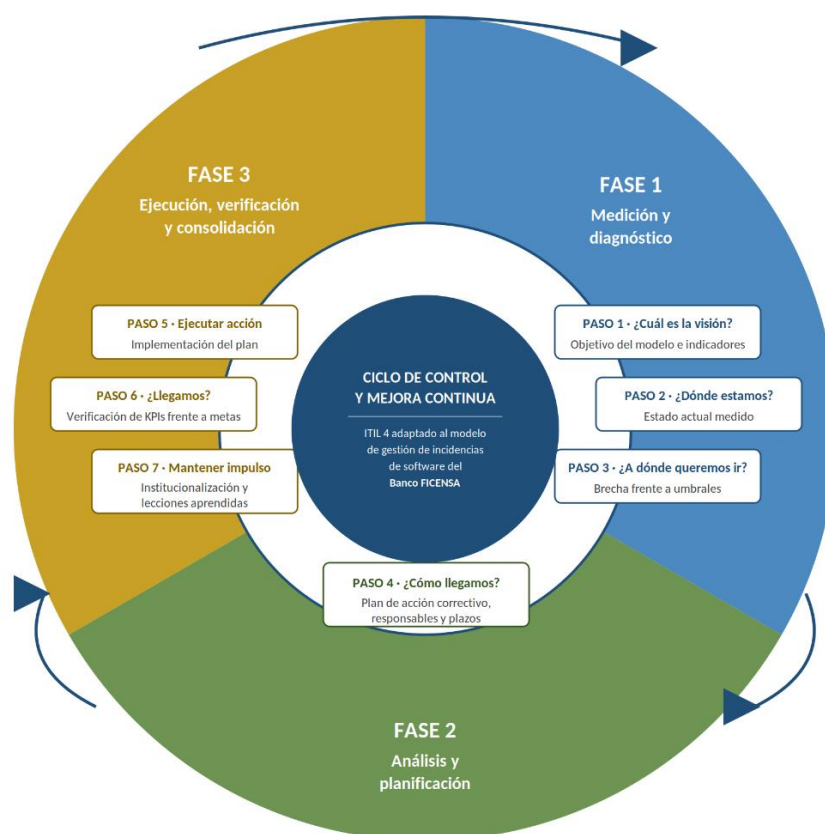


Figura 36. Ciclo de control del modelo.

Fuente: Elaboración propia.

6.5.3. ACCIONES ANTE DESVIACIÓN

Las acciones ante desviación se activan cuando los indicadores del tablero de KPIs muestran un comportamiento fuera del rango esperado o una tendencia de deterioro respecto al período anterior. Esta lógica se armoniza con la semaforización definida en la matriz de acuerdos de nivel de servicio, de manera que el modelo mantenga una lectura común entre el seguimiento operativo del ticket y el control institucional de los indicadores. Mientras la semaforización de SLA opera sobre el consumo de tiempo de cada ticket, la presente tabla aplica sobre los resultados consolidados del tablero de KPIs.

Acciones ante desviación con umbrales automáticos de activación



Zona de desempeño	Umbral automático de activación	Indicadores de referencia	Acción automática o institucional	Responsable de seguimiento
Verde	- El indicador se mantiene dentro del rango aceptable definido - Registro formal $\geq 95\%$ - Tiempo administrativo del primer nivel $\geq 90\%$ - Cumplimiento del SLA técnico $\geq 85\%$ - MTTR conforme al SLA por prioridad - Reincidencia $\geq 20\%$ - Trazabilidad completa $\geq 90\%$ - Satisfacción del usuario ≥ 4.0 de 5.0	• Todos los KPIs del tablero.	• Registro ordinario del resultado en el tablero, sin alerta adicional. • Se mantiene la operación normal del modelo.	Responsable operativo del indicador.
Amarilla	- El indicador permanece dentro del rango aceptable, pero muestra deterioro frente al período anterior - Disminución de 5 puntos porcentuales o más en indicadores de cumplimiento - Aumento de 10% o más en MTTR o reincidencia, o alerta amarilla de SLA - Por consumo mayor al 50% y hasta el 75% del tiempo objetivo en tickets activos	• Registro formal • Cumplimiento administrativo • SLA técnico • MTTR • Reincidencia • Trazabilidad • Satisfacción	• Alerta preventiva en el tablero. • Revisión de causa probable y seguimiento por el Jefe de Proyectos y Desarrollo.	Jefe de Proyectos y Desarrollo.
Naranja	- El indicador se ubica en proximidad de incumplimiento: registro formal entre 95% y 96% - Tiempo administrativo entre 90% y 92% - SLA técnico entre 85% y 87% - Reincidencia entre 18% y 20% - Trazabilidad entre 90% y 92% - Satisfacción entre 4.0 y 4.2 - O tickets activos con consumo mayor al 75% y hasta el 90% del SLA	• Indicadores con límite mínimo, límite máximo o SLA aplicable.	• Alerta de riesgo en el tablero. • Notificación anticipada al responsable operativo y solicitud de acción correctiva inmediata.	Jefe de Proyectos y Desarrollo y responsable operativo del indicador.
Roja	- El indicador incumple el límite aceptable: registro formal $< 95\%$ - Tiempo administrativo $< 90\%$ - SLA técnico $< 85\%$ - MTTR superior al SLA aplicable por prioridad - Reincidencia $> 20\%$ - Trazabilidad $< 90\%$ - Satisfacción < 4.0 - O tickets activos con vencimiento del SLA al 100% del tiempo objetivo.	• Todos los KPIs con límite definido.	• Registro de desviación formal. • Elaboración de plan de acción correctivo con responsable, plazo y evidencia de seguimiento.	Jefe de Proyectos y Desarrollo.
Negra / Crítica	- La desviación roja se repite durante dos períodos consecutivos, afecta un sistema crítico, compromete continuidad operativa, genera posible afectación regulatoria o corresponde a incumplimiento de SLA en un caso crítico institucionalmente reportable.	• SLA técnico • MTTR • Reincidencia • Trazabilidad • Sistemas críticos • Eventos con impacto regulatorio o de continuidad.	• Escalamiento institucional automático, notificación a la Gerencia de Tecnología y Comunicaciones y activación de seguimiento gerencial o comité extraordinario.	Gerente de Tecnología y Comunicaciones, con apoyo del Jefe de Proyectos y Desarrollo.

Figura 37. Umbrales automáticos de activación ante desviaciones del tablero de KPIs.

Fuente: Elaboración propia.

6.5.4. ROLES DE SUPERVISIÓN DEL CONTROL

La supervisión del control del modelo se ejecutará mediante una estructura escalonada de seguimiento, integrada por niveles operativo, táctico y gerencial. Esta organización permite revisar los indicadores según su naturaleza, asegurar continuidad en el monitoreo del proceso y escalar oportunamente las desviaciones que excedan la capacidad de control del nivel inmediato.

En condiciones normales, el seguimiento se realizará a través de comités con periodicidad definida; sin embargo, cuando se active una desviación crítica o un evento con impacto en continuidad operativa, sistemas críticos o cumplimiento institucional, podrá convocarse un comité extraordinario para la toma inmediata de decisiones.

Tabla 62. Roles de supervisión de indicadores.

Rol	Función en el control	Comité de seguimiento	Periodicidad	Evidencia esperada
Oficial de Soporte Proyectos / Help Desk	Consolida y verifica los datos operativos de incidencias generales, registro formal, tiempos administrativos y estados de tickets.	Comité operativo	Semanal	Reporte operativo de tickets, backlog, tickets en riesgo y cumplimiento administrativo.
Oficial de Soporte Cash Management	Consolida y verifica los datos operativos asociados a incidencias del sistema Cash Management.	Comité operativo	Semanal	Reporte operativo de incidencias, estado de tickets y cumplimiento administrativo del sistema.
Analista Programador Senior	Supervisa incidencias críticas, reincidencias, tickets escalados y casos vinculados a Gestión de Problemas.	Comité operativo y comité táctico	Semanal y mensual	Bitácora técnica, análisis de reincidencia, tickets-problema vinculados y seguimiento de casos críticos.
Jefe de Proyectos y Desarrollo	Consolida KPIs, analiza desviaciones, coordina acciones correctivas y da seguimiento al cumplimiento del modelo.	Comité táctico	Mensual	Informe consolidado de KPIs, análisis de desviaciones y plan de acción correctivo.
Gerente de Tecnología y Comunicaciones	Evalúa resultados estratégicos, desviaciones críticas, decisiones estructurales y requerimientos de ajuste del modelo.	Comité gerencial	Trimestral	Acta de comité gerencial, decisiones adoptadas y seguimiento a medidas estructurales.
Auditoría Interna	Verifica la consistencia de la trazabilidad documental y la integridad de los registros de control.	Comité táctico o revisión programada	Trimestral	Informe de revisión, observaciones y recomendaciones de control.

Rol	Función en el control	Comité de seguimiento	Periodicidad	Evidencia esperada
Coordinador de Continuidad del Negocio y Riesgo Tecnológico*	Participa cuando existan desviaciones críticas, afectación a sistemas críticos, continuidad operativa o eventos institucionalmente reportables.	Comité extraordinario	A requerimiento	Acta extraordinaria, evaluación de impacto y medidas institucionales de respuesta.

Fuente: Elaboración propia.

6.6. CRONOGRAMA DE IMPLEMENTACIÓN

La implementación del modelo propuesto se plantea mediante un cronograma dividido en siete fases. Esta estructura permite organizar el trabajo de forma progresiva, desde la preparación institucional hasta el seguimiento inicial de los indicadores de desempeño. La propuesta no contempla la adquisición de una nueva herramienta tecnológica, debido a que Banco FICENSA ya dispone de ManageEngine ServiceDesk Plus como plataforma institucional. Por tanto, el esfuerzo principal se concentra en formalizar el proceso, configurar el flujo, capacitar a los usuarios, validar su funcionamiento y medir los resultados iniciales.

El cronograma se estima para un período de doce semanas y se estructura en siete fases secuenciales. Cada fase incorpora tareas específicas, responsables, productos esperados, hitos de validación y acciones de gestión del cambio. La inclusión de estos elementos permite verificar el avance antes de pasar a la siguiente etapa, reducir la resistencia de los usuarios, asegurar la correcta adopción del flujo formal y evitar que la implementación se limite únicamente a la configuración técnica de la herramienta.

Tabla 63: Cronograma de implementación del modelo propuesto

Fase	Período estimado	Tareas específicas	Hito de validación y gestión del cambio	Responsable principal	Responsables de apoyo	Producto esperado
Fase 1. Preparación y aprobación inicial	Semana 1	1. Presentar el modelo propuesto a la Gerencia de Tecnología y Comunicaciones. 2. Revisar los hallazgos principales del diagnóstico: informalidad del registro, falta de trazabilidad, reincidencia y tiempos variables de atención. 3. Confirmar que el alcance aplica únicamente a incidencias de software de Negocios y Operaciones. 4. Validar que la implementación se realizará sobre ManageEngine ServiceDesk Plus. 5. Obtener aprobación inicial para iniciar la configuración del modelo.	Hito de validación: aprobación formal del alcance, responsables y autorización inicial. Gestión del cambio: comunicación inicial a los actores clave sobre el propósito del modelo, beneficios esperados y alcance de la implementación.	Gerente de Tecnología y Comunicaciones	Jefe de Proyectos y Desarrollo; Oficial de Soporte Proyectos / Help Desk; Oficial de Soporte Cash Management	Alcance aprobado, actores clave informados y autorización inicial para continuar con el diseño operativo.

Fase	Período estimado	Tareas específicas	Hito de validación y gestión del cambio	Responsable principal	Responsables de apoyo	Producto esperado
Fase 2. Socialización con áreas usuarias y técnicas	Semana 2	1. Socializar el propósito del modelo con usuarios clave de Negocios y Operaciones. 2. Explicar que toda incidencia de software deberá convertirse en ticket formal. 3. Presentar los roles generales del colaborador reportante, Mesa de Servicio, Desarrollo y jefaturas. 4. Recopilar observaciones de las áreas usuarias sobre campos necesarios, sistemas críticos y dificultades actuales de reporte. 5. Ajustar el enfoque del flujo según retroalimentación operativa razonable.	Hito de validación: validación de necesidades operativas de usuarios clave. Gestión del cambio: sensibilización inicial sobre el nuevo esquema de registro formal y recopilación de inquietudes para reducir resistencia al cambio.	Jefe de Proyectos y Desarrollo	Oficial de Soporte Proyectos / Help Desk; Oficial de Soporte Cash Management; usuarios clave de Negocios y Operaciones	Áreas usuarias enteradas del cambio, observaciones recopiladas y necesidades operativas consideradas antes de la configuración.
Fase 3. Diseño detallado del flujo y responsabilidades	Semanas 3 y 4	1. Revisar las siete etapas del flujo: registro, validación, clasificación, priorización, asignación, diagnóstico y	Hito de validación: aprobación del flujo operativo, etapas, responsables y	Jefe de Proyectos y Desarrollo	Oficial de Soporte Proyectos / Help Desk; Oficial de Soporte Cash Management;	Flujo detallado, responsabilidades validadas y matriz de roles lista para incorporarse al

Fase	Período estimado	Tareas específicas	Hito de validación y gestión del cambio	Responsable principal	Responsables de apoyo	Producto esperado
		resolución, validación y cierre. 2. Definir qué información entra y qué información sale de cada etapa. 3. Establecer condiciones para avanzar de una etapa a otra. 4. Revisar la Matriz RA/RACI y confirmar responsables por actividad. 5. Definir qué casos serán atendidos por Soporte Proyectos / Help Desk y cuáles por Soporte Cash Management. 6. Establecer cuándo interviene el Analista Programador Senior, los Analistas Programadores Junior, el Jefe de Proyectos y Desarrollo y el Gerente de Tecnología y Comunicaciones.	matriz de roles antes de configurar la herramienta. Gestión del cambio: revisión conjunta con Mesa de Servicio, Desarrollo y áreas usuarias para asegurar comprensión del nuevo flujo y responsabilidades.		Analista Programador Senior; Analistas Programadores Junior	procedimiento operativo.

Fase	Período estimado	Tareas específicas	Hito de validación y gestión del cambio	Responsable principal	Responsables de apoyo	Producto esperado
Fase 4. Definición de campos, criticidad, SLA y reglas de escalamiento	Semana 5	1. Definir los campos obligatorios del ticket: usuario reportante, área afectada, sistema, módulo, descripción de la falla, evidencia adjunta, impacto, urgencia y afectación a otros usuarios. 2. Validar las categorías y subcategorías de incidencias de software. 3. Configurar criterios de criticidad según impacto y urgencia. 4. Definir tiempos objetivo de atención y resolución por nivel de criticidad. 5. Establecer reglas de escalamiento funcional y jerárquico. 6. Definir cuándo un caso reincidente debe enviarse a análisis de causa raíz o gestión de problemas.	Hito de validación: aprobación de campos obligatorios, criterios de criticidad, SLA y reglas de escalamiento. Gestión del cambio: explicación a usuarios y responsables técnicos sobre la información mínima requerida y la forma en que se priorizarán las incidencias.	Oficial de Soporte Proyectos / Help Desk	Oficial de Soporte Cash Management; Jefe de Proyectos y Desarrollo; Analista Programador Senior; Gerente de Tecnología y Comunicaciones	Campos obligatorios definidos, matriz de criticidad validada, SLA preliminares establecidos y reglas de escalamiento documentadas.

Fase	Período estimado	Tareas específicas	Hito de validación y gestión del cambio	Responsable principal	Responsables de apoyo	Producto esperado
Fase 5. Configuración en ManageEngine ServiceDesk Plus	Semanas 6 y 7	1. Definir los campos obligatorios del ticket: usuario reportante, área afectada, sistema, módulo, descripción de la falla, evidencia adjunta, impacto, urgencia y afectación a otros usuarios. 2. Validar las categorías y subcategorías de incidencias de software. 3. Configurar criterios de criticidad según impacto y urgencia. 4. Definir tiempos objetivo de atención y resolución por nivel de criticidad. 5. Establecer reglas de escalamiento funcional y jerárquico. 6. Definir cuándo un caso reincidente debe enviarse a análisis de causa raíz o gestión de problemas.	Hito de validación: validación técnica del flujo configurado en ManageEngine ServiceDesk Plus antes del piloto. Gestión del cambio: pruebas internas guiadas con Mesa de Servicio y Desarrollo para familiarizar a los responsables con el flujo configurado.	Oficial de Soporte Proyectos / Help Desk	Oficial de Soporte Cash Management; Analista Programador Senior; Analistas Programadores Junior; Jefe de Proyectos y Desarrollo	Flujo configurado en la plataforma, formulario operativo, reglas parametrizadas, pruebas internas ejecutadas y reportes básicos disponibles para seguimiento.

Fase	Período estimado	Tareas específicas	Hito de validación y gestión del cambio	Responsable principal	Responsables de apoyo	Producto esperado
Fase 6. Capacitación y prueba piloto	Semanas 8 y 9	1. Capacitar a usuarios clave de Negocios y Operaciones sobre el registro de incidencias en la Mesa de Servicio. 2. Explicar qué información mínima debe completar el usuario. 3. Capacitar a Mesa de Servicio sobre validación, clasificación, priorización y asignación. 4. Capacitar a Desarrollo sobre diagnóstico, documentación de solución y cierre técnico. 5. Ejecutar piloto con un grupo controlado de usuarios o con sistemas de mayor reincidencia. 6. Registrar incidencias reales o simuladas.	Hito de validación: aprobación del piloto y validación de que el flujo funciona antes de la puesta en marcha general. Gestión del cambio: capacitación práctica, acompañamiento a usuarios clave y recopilación de retroalimentación para ajustar el proceso antes de su habilitación general.	Jefe de Proyectos y Desarrollo	Oficial de Soporte Proyectos / Help Desk; Oficial de Soporte Cash Management; Analista Programador Senior; Analistas Programadores Junior; usuarios clave de Negocios y Operaciones	Usuarios capacitados, piloto ejecutado, retroalimentación recopilada, ajustes aplicados y flujo corregido antes de la puesta en marcha general.

Fase	Período estimado	Tareas específicas	Hito de validación y gestión del cambio	Responsable principal	Responsables de apoyo	Producto esperado
		7. Verificar si el ticket conserva trazabilidad completa. 8. Identificar errores de configuración, campos innecesarios o información faltante. 9. Ajustar formulario, reglas de asignación, prioridades o SLA según resultados del piloto.				
Fase 7. Puesta en marcha, seguimiento y mejora inicial	Semanas 10 a 12	1. Habilitar el flujo formal para todas las incidencias de software de Negocios y Operaciones. 2. Comunicar que ManageEngine ServiceDesk Plus será el medio oficial de registro. 3. Dar acompañamiento inicial a usuarios y responsables técnicos. 4. Revisar semanalmente los tickets registrados.	Hito de validación: validación de resultados iniciales mediante revisión de tickets, KPIs e informe gerencial. Gestión del cambio: acompañamiento posterior a la puesta en marcha, resolución de dudas, refuerzo del canal oficial y ajustes tempranos	Gerente de Tecnología y Comunicaciones	Jefe de Proyectos y Desarrollo; Oficial de Soporte Proyectos / Help Desk; Oficial de Soporte Cash Management; Anali	

Fase	Período estimado	Tareas específicas	Hito de validación y gestión del cambio	Responsable principal	Responsables de apoyo	Producto esperado
		5. Verificar que los casos tengan clasificación, prioridad, responsable, solución y cierre documentado. 6. Calcular los primeros KPIs: porcentaje de registros formales, tiempo de atención, tiempo de resolución, reincidencia, cumplimiento de SLA y cierre documentado. 7. Identificar incidencias repetidas que deban escalarse a gestión de problemas. 8. Presentar un informe inicial de resultados a la Gerencia de Tecnología y Comunicaciones.	con base en la experiencia real de uso.			

Fuente: Elaboración propia.

El cronograma propuesto responde a una lógica de implementación secuencial tipo cascada, en la cual cada fase toma como base los entregables de la etapa anterior para avanzar de manera ordenada. Esta estructura permite controlar mejor el alcance, validar los resultados por etapa y reducir el riesgo de configurar o habilitar el flujo sin haber definido previamente las responsabilidades, campos obligatorios, criterios de criticidad y reglas de escalamiento. Las primeras fases se enfocan en la aprobación, socialización y diseño detallado del modelo; las fases intermedias se orientan a configurar la plataforma y validar su funcionamiento; y la fase final permite poner en marcha el proceso con seguimiento inicial de indicadores.

La prueba piloto representa un punto de control dentro de esta implementación secuencial, ya que permite validar el modelo antes de extenderlo a toda la operación. En esta etapa se recomienda seleccionar usuarios de Negocios y Operaciones, así como sistemas que hayan presentado mayor recurrencia durante el diagnóstico. Esto permitirá verificar si los campos del ticket son comprensibles, si la clasificación resulta práctica, si la asignación llega al responsable correcto y si los tiempos objetivo son razonables para la operación real del banco.

Una vez implementado el modelo, el seguimiento inicial deberá realizarse semanalmente durante el primer mes. Esta revisión permitirá confirmar si las incidencias están ingresando por el canal formal, si los tickets contienen la información mínima requerida, si el área de Desarrollo documenta adecuadamente la solución y si existen casos reincidentes que deban analizarse como problemas. De esta forma, la implementación no se limita a habilitar un formulario en la herramienta, sino que busca consolidar un proceso trazable, medible y alineado con ITIL 4.

A continuación, se presenta una tabla tipo calendario que resume la distribución semanal de las fases de implementación.

Tabla 64: Resumen del cronograma de implementación

Fase / Semana	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12
Fase 1. Preparación y aprobación inicial	X											
Fase 2. Socialización con áreas usuarias y técnicas		X										
Fase 3. Diseño detallado del flujo y responsabilidades			X	X								
Fase 4. Definición de campos, criticidad, SLA y escalamiento					X							
Fase 5. Configuración en ManageEngine ServiceDesk Plus						X	X					
Fase 6. Capacitación y prueba piloto								X	X			
Fase 7. Puesta en marcha, seguimiento y mejora inicial										X	X	X

Fuente: Elaboración propia.

6.7. PRESUPUESTO E IMPACTO DEL PRESUPUESTO

6.7.1. CONSIDERACIONES GENERALES DEL PRESUPUESTO

La implementación del modelo requiere considerar los recursos tecnológicos, operativos, humanos y financieros necesarios para su puesta en marcha en Banco FICENSA. La propuesta utilizará ManageEngine ServiceDesk Plus, plataforma que actualmente forma parte de la infraestructura tecnológica institucional, para formalizar el registro, clasificación y seguimiento de las incidencias de software.

Debido a que la solución funcionará bajo un esquema local o on-premises, será necesario verificar si la infraestructura existente dispone de capacidad suficiente para soportar la configuración propuesta, el almacenamiento de tickets y archivos adjuntos, así como la generación de reportes e indicadores.

Si la infraestructura existente cumple con las especificaciones requeridas, no será necesario adquirir un servidor nuevo. Cuando la capacidad resulte insuficiente, deberá provisionarse una máquina virtual adicional o adquirirse un servidor físico que cumpla con los requerimientos definidos para la plataforma.

Para efectos del análisis financiero, los costos se clasifican en existentes e incrementales. Los costos existentes corresponden a recursos que Banco FICENSA mantiene independientemente de la propuesta, como el licenciamiento anual de ManageEngine ServiceDesk Plus.

Los costos incrementales comprenden únicamente los desembolsos adicionales atribuibles a la implementación. Estos incluyen el soporte técnico especializado y, cuando resulte necesario, el provisionamiento o adquisición de infraestructura tecnológica adicional.

Tabla 65: Requisitos técnicos para la implementación de ManageEngine ServiceDesk Plus

Requisito	Especificación requerida	Descripción
Tipo de servicio	Local (<i>on-premises</i>)	Utilización de infraestructura administrada por el banco, sujeta a la validación de su capacidad disponible.
Sistema operativo	Windows Server	Plataforma base para la instalación y operación del servicio.
Memoria RAM	16 GB	Capacidad estimada para mantener una operación estable de la aplicación.

Requisito	Especificación requerida	Descripción
Almacenamiento	500 GB	Espacio destinado a la instalación, base de datos, archivos adjuntos, registros y crecimiento operativo.
Procesamiento	4 CPU	Capacidad estimada para procesar solicitudes, consultas, automatizaciones y reportes.

Fuente: Elaboración propia con base en los requerimientos técnicos de ManageEngine ServiceDesk Plus..

Las especificaciones presentadas constituyen una referencia para la planificación presupuestaria. Antes de la implementación deberán validarse según la versión de ServiceDesk Plus instalada, la cantidad proyectada de técnicos y usuarios, el volumen de tickets, el crecimiento de los archivos adjuntos y la capacidad disponible en la infraestructura institucional.

6.7.2. PRESUPUESTO ESTIMADO DE IMPLEMENTACIÓN

La implementación del modelo requiere recursos para la configuración del flujo, parametrización de campos, establecimiento de reglas de criticidad, configuración de SLA, elaboración de reportes, ejecución de pruebas y acompañamiento durante la puesta en marcha.

El presupuesto diferencia los recursos existentes de los costos incrementales. Esta separación evita considerar como inversión nueva los recursos que Banco FICENSA mantiene como parte de su operación tecnológica habitual.

El soporte técnico especializado se estima en 40 horas, con una tarifa referencial de USD 70 por hora. Asimismo, se incorpora un costo de planificación de USD 3,500 para un servidor físico, aplicable únicamente cuando la infraestructura existente no disponga de capacidad suficiente.

Tabla 66: Presupuesto estimado de implementación

Concepto	Clasificación	Costo estimado	Tratamiento financiero
Licenciamiento anual de ServiceDesk Plus	Costo existente	USD 23,639	Costo operativo existente excluido de la inversión incremental.
Soporte técnico especializado	Costo incremental	USD 2,800	Corresponde a 40 horas a una tarifa de USD 70 por hora.
Servidor físico de referencia	Costo incremental	USD 3,500	Estimación de planificación sujeta a cotización formal.
Memoria, almacenamiento y procesamiento	Incluido	USD 0	Componentes incluidos en el costo estimado del servidor.
Inversión incremental estimada	—	USD 6,300	Base empleada para el cálculo del ROI.

Concepto	Clasificación	Costo estimado	Tratamiento financiero
Recursos económicos totales del primer año	—	USD 29,939	Incluye los costos existentes e incrementales.

Fuente: Elaboración propia.

La inversión incremental asciende a USD 6,300, integrada por USD 2,800 de soporte especializado y USD 3,500 como costo referencial del servidor. El licenciamiento anual de USD 23,639 se clasifica como costo existente, debido a que Banco FICENSA ya utiliza la plataforma.

El costo referencial del servidor constituye un supuesto de planificación. Antes de la implementación deberá validarse mediante cotizaciones de proveedores autorizados. Si el banco dispone de capacidad en su infraestructura virtual, este desembolso podría reducirse o eliminarse.

6.7.3. JUSTIFICACIÓN DEL PRESUPUESTO

El componente de mayor valor dentro de los recursos económicos totales corresponde al licenciamiento anual de ManageEngine ServiceDesk Plus. Sin embargo, este constituye un costo existente, debido a que la plataforma ya forma parte de la infraestructura tecnológica de Banco FICENSA.

Por consiguiente, el licenciamiento no representa un desembolso adicional generado por la propuesta y se excluye de la inversión incremental utilizada para calcular el ROI. Su inclusión en el presupuesto permite mostrar el total de recursos económicos relacionados con la operación de la plataforma.

El soporte técnico constituye un costo incremental necesario para configurar el flujo, los campos obligatorios, las reglas de criticidad, los SLA, los reportes, las pruebas y los controles definidos en el modelo. También se contempla infraestructura adicional cuando la capacidad existente resulte insuficiente.

La propuesta aprovecha una plataforma disponible y concentra la inversión incremental en la formalización del proceso. Esto permite mejorar la trazabilidad, controlar los tiempos de atención y resolución, reducir la informalidad y fortalecer la toma de decisiones basada en información verificable.

6.7.4. ANÁLISIS FINANCIERO ESTIMADO DE LA PROPUESTA

El análisis financiero se desarrolla considerando la inversión incremental, la continuidad de los servicios soportados por software y la reducción de reprocesos. Los beneficios no representan ingresos nuevos garantizados, sino valores que podrían preservarse o costos operativos que podrían evitarse.

Los sistemas analizados soportan servicios operativos y transaccionales relacionados con ENEE, AMDC, AMSPS, matrícula vehicular, Hondutel y RAP, entre otros. Las fallas o interrupciones en estos sistemas pueden afectar el procesamiento de operaciones, producir reprocesos y limitar la continuidad del servicio.

El modelo también genera beneficios regulatorios y de control interno mediante el registro de responsables, fechas, prioridades, escalamientos, acciones ejecutadas y evidencia de cierre. No obstante, estos beneficios se presentan de manera cualitativa y se excluyen del ROI para evitar una sobreestimación.

La estimación financiera considera únicamente los beneficios cuantificables relacionados con las comisiones potencialmente preservadas y la reducción de reprocesos. El análisis utiliza un horizonte de dos años, aunque el período estimado de recuperación puede producirse durante el primer año.

6.7.5. BENEFICIOS ECONÓMICOS ESPERADOS

La estimación utiliza una inversión incremental de USD 6,300. Los beneficios económicos corresponden a la continuidad de los servicios soportados por software y a la reducción del esfuerzo dedicado a reprocesos operativos.

Las comisiones preservadas se estiman considerando un valor mensual referencial de operaciones que podrían dejar de procesarse debido a interrupciones. El ahorro por reprocesos se calcula a partir del esfuerzo operativo y técnico que podría evitarse al mejorar el registro, seguimiento y escalamiento de las incidencias.

Los valores utilizados constituyen supuestos de planificación. Antes de la implementación deberán validarse con datos institucionales sobre operaciones afectadas, comisiones por transacción, horas destinadas a reprocesos y costo promedio del personal involucrado.

Los beneficios regulatorios, la evidencia para auditoría, la trazabilidad, la reportería, la satisfacción del usuario y la madurez institucional no se monetizan. Estos elementos se presentan como beneficios cualitativos y se excluyen del cálculo del ROI.

Tabla 67: Supuestos económicos, regulatorios y de procesos internos para la estimación

Componente	Supuesto utilizado	Forma de estimación	Tipo de beneficio
Servicios comisionables soportados por software	Continuidad de pagos y recaudaciones vinculados a ENEE, AMDC, AMSPS, matrícula vehicular, Hondutel, RAP, entre otros.	Comisiones que podrían preservarse al reducir interrupciones o fallas en servicios transaccionales.	Económico
Reprocesos por fallas de software	Menor cantidad de operaciones revisadas, corregidas o gestionadas manualmente por errores del sistema.	Tiempo operativo y técnico evitado por menor cantidad de fallas recurrentes.	Económico y operativo
Mitigación regulatoria	Mayor trazabilidad y disponibilidad de evidencia sobre las incidencias	Valoración cualitativa excluida del cálculo del ROI	Regulatorio y cualitativo
Evidencia para auditoría	Disponibilidad de registros formales sobre atención, responsables, fechas, acciones y cierre de incidencias.	Horas evitadas en reconstrucción de información dispersa en correos, llamadas o mensajes.	Proceso interno
Mejora de trazabilidad	Registro centralizado del ciclo de vida de cada incidencia.	Reducción de casos sin seguimiento formal y mayor control de estados.	Proceso interno
Reportería e indicadores	Generación oportuna de reportes, KPIs y tableros de control.	Menor esfuerzo manual para consolidar información y mejor toma de decisiones.	Proceso interno
Satisfacción del usuario	Mayor claridad sobre el estado, responsable y avance de cada incidencia.	Beneficio cualitativo asociado a experiencia del usuario interno.	Cualitativo
Madurez institucional	Formalización del proceso de gestión de incidencias de software.	Mayor alineación con buenas prácticas de gobierno de TI y mejora continua.	Cualitativo

Fuente: Elaboración propia

6.7.6. BENEFICIOS ECONÓMICOS ESTIMADOS POR CONTINUIDAD DE SOFTWARE

El primer beneficio económico corresponde a las comisiones que podrían preservarse mediante la continuidad de los servicios de pago y recaudación soportados por software. Estos servicios dependen de aplicaciones internas, integraciones tecnológicas y procesos operativos para completar las transacciones.

Para el primer año se utiliza un supuesto de USD 700 mensuales en comisiones potencialmente preservadas, equivalente a USD 8,400 anuales. Para el segundo año se considera

un valor de USD 900 mensuales, equivalente a USD 10,800 anuales.

El segundo beneficio corresponde a la reducción de reprocesos relacionados con operaciones afectadas, corrección de inconsistencias y seguimiento manual de incidencias. Se estiman USD 200 mensuales durante el primer año y USD 250 mensuales durante el segundo.

Tabla 68. Beneficios económicos por continuidad de software.

Beneficio	Año 1	Año 2	Base de cálculo
Comisiones potencialmente preservadas	USD 8,400	USD 10,800	Año 1: USD 700 × 12. Año 2: USD 900 × 12.
Reducción de reprocesos	USD 2,400	USD 3,000	Año 1: USD 200 × 12. Año 2: USD 250 × 12.
Total estimado	USD 10,800	USD 13,800	Valores referenciales sujetos a validación institucional.

Fuente: Elaboración propia.

Los valores mensuales constituyen supuestos de planificación y deberán validarse con información de las áreas de Finanzas, Operaciones y Recursos Humanos. La validación deberá considerar las comisiones promedio, las operaciones afectadas, las horas destinadas a reprocesos y el costo promedio del personal.

6.7.7. BENEFICIOS ESPERADOS POR MITIGACIÓN REGULATORIA

La mitigación regulatoria constituye un beneficio cualitativo relacionado con el fortalecimiento de la trazabilidad, la conservación de evidencia y la capacidad institucional para demostrar control sobre las incidencias de software.

La propuesta contribuye a este beneficio mediante el registro centralizado, la clasificación por criticidad, las reglas de escalamiento, la asignación de responsables, el seguimiento de tiempos y la documentación del cierre.

Estos elementos facilitan la presentación de evidencia ante auditorías, revisiones internas o requerimientos de los entes supervisores. Sin embargo, no se asigna un valor monetario a las sanciones potencialmente evitadas.

No existe evidencia suficiente para relacionar directamente las incidencias analizadas con una infracción determinada, una sanción aplicable o un número específico de días de incumplimiento. Por esta razón, la mitigación regulatoria se excluye del cálculo del ROI.

6.7.8. BENEFICIOS DE PROCESOS INTERNOS Y CUALITATIVOS

Además de los beneficios económicos cuantificables, la propuesta genera beneficios de procesos internos y cualitativos que fortalecen la gestión institucional. Estos beneficios no se incorporan directamente en el cálculo monetario del ROI para evitar una sobreestimación financiera, pero sí forman parte del valor integral de la propuesta.

Uno de los principales beneficios corresponde al fortalecimiento de la trazabilidad. Al centralizar el registro de incidencias en una herramienta formal, el banco podrá identificar el origen del caso, usuario reportante, sistema afectado, prioridad asignada, técnico responsable, acciones ejecutadas, tiempos de atención y cierre.

Otro beneficio relevante es la mejora en la generación de reportes e indicadores. El modelo permite disponer de información consolidada para medir tiempos de atención, tiempos de resolución, reincidencia, cumplimiento de SLA, criticidad de los casos y desempeño del proceso, lo cual facilita la toma de decisiones basada en datos.

La propuesta también contribuye a mejorar la satisfacción del usuario interno, debido a que los colaboradores podrán contar con un canal formal, seguimiento visible, notificaciones y mayor claridad sobre el estado de sus solicitudes. Esto reduce la incertidumbre operativa y mejora la percepción del servicio brindado por el área de TI.

Finalmente, el modelo fortalece la madurez institucional del proceso de gestión de incidencias de software. La existencia de roles, reglas, indicadores, matriz de criticidad, acuerdos de nivel de servicio y controles de seguimiento permite avanzar hacia una gestión más ordenada, medible y alineada con buenas prácticas de gobierno de TI.

Tabla 69. Beneficios de procesos internos y cualitativos.

Beneficio	Descripción	Impacto esperado
Mayor trazabilidad	Registro completo del ciclo de vida de cada incidencia.	Mejor control operativo y mayor evidencia institucional.
Mejor seguimiento de incidencias	Visibilidad sobre estado, responsable, prioridad y tiempo de atención.	Reducción de casos sin control o sin cierre documentado.

Reportes e indicadores oportunos	Generación de KPIs y tableros de seguimiento.	Mejor toma de decisiones y control gerencial.
Mejora de satisfacción del usuario	Mayor claridad sobre el avance de las solicitudes.	Mejor percepción del servicio interno de TI.
Madurez del proceso	Formalización de roles, reglas, etapas, SLA y controles.	Fortalecimiento del gobierno de TI.
Fortalecimiento reputacional	Mayor capacidad institucional para demostrar control y continuidad.	Confianza interna y mejor respuesta ante auditorías.

Fuente: Elaboración propia.

6.7.9. ESCENARIO DE RECUPERACIÓN DE LA INVERSIÓN A DOS AÑOS (ROI)

Después de excluir la estimación monetaria de las sanciones, los beneficios económicos corresponden únicamente a la continuidad de servicios y la reducción de reprocesos. El beneficio estimado asciende a USD 10,800 durante el primer año y USD 13,800 durante el segundo, para un beneficio acumulado de USD 24,600.

Al comparar el beneficio acumulado de USD 24,600 con la inversión incremental de USD 6,300, se obtiene un beneficio neto estimado de USD 18,300 al cierre del segundo año. Este resultado es referencial y deberá actualizarse cuando Banco FICENSA valide los costos y beneficios utilizados.

Tabla 70. Recuperación de la inversión por año.

Periodo	Beneficio anual	Beneficio acumulado	Saldo frente a la inversión
Inversión inicial	USD 0	USD 0	-USD 6,300
Año 1	USD 10,800	USD 10,800	USD 4,500
Año 2	USD 13,800	USD 24,600	USD 18,300

Fuente: Elaboración propia.

6.7.10. CÁLCULO DEL RETORNO DE INVERSIÓN

El retorno de inversión se calcula comparando los beneficios económicos acumulados con la inversión incremental estimada. El cálculo incorpora únicamente los beneficios relacionados con la continuidad de los servicios soportados por software y la reducción de reprocesos, excluyendo la mitigación regulatoria y los demás beneficios cualitativos.

La fórmula aplicada es la siguiente:

$$ROI \text{ acumulado} = [(Beneficio \text{ acumulado} - Inversión \text{ incremental}) / Inversión \text{ incremental}] \times 100$$

Aplicando el escenario de dos años:

$$\text{ROI acumulado} = [(\text{USD } 24,600 - \text{USD } 6,300) / \text{USD } 6,300] \times 100$$

$$\text{ROI acumulado} = 290.48\%$$

El porcentaje obtenido responde a que la plataforma ya existe en Banco FICENSA y el análisis considera únicamente los costos incrementales necesarios para implementar el modelo. El resultado deberá interpretarse como una estimación referencial, condicionada a la validación de los beneficios y del costo definitivo del servidor.

6.7.11. PERÍODO DE RECUPERACIÓN DE LA INVERSIÓN

Durante el primer año se proyecta un beneficio económico de USD 10,800. Este monto equivale a un beneficio promedio mensual de USD 900, obtenido al dividir el beneficio anual estimado entre los doce meses del año.

Al dividir la inversión incremental de USD 6,300 entre el beneficio promedio mensual de USD 900, se obtiene un período estimado de recuperación de siete meses. Por consiguiente, bajo el escenario base, la inversión podría recuperarse dentro del primer año de operación del modelo.

Este resultado constituye una estimación referencial. El período de recuperación deberá actualizarse cuando se disponga de la cotización definitiva del servidor y de información institucional que permita validar las comisiones potencialmente preservadas y la reducción de reprocesos.

6.7.12. ANÁLISIS DE SENSIBILIDAD

El análisis de sensibilidad permite evaluar el comportamiento financiero de la propuesta ante variaciones en los beneficios económicos estimados. Para ello, se establecen tres escenarios: conservador, base y favorable, manteniendo una inversión incremental de USD 6,300.

El escenario conservador contempla una reducción del 20% en los beneficios proyectados. El escenario base conserva las estimaciones utilizadas en el análisis financiero, mientras que el escenario favorable considera un incremento del 20%.

Tabla 71. Análisis de sensibilidad de la propuesta

Escenario	Beneficio año 1	Beneficio año 2	Beneficio acumulado	ROI acumulado	Recuperación estimada
Conservador (-20%)	USD 8,640	USD 11,040	USD 19,680	212.38%	8.75 meses

Escenario	Beneficio año 1	Beneficio año 2	Beneficio acumulado	ROI acumulado	Recuperación estimada
Base	USD 10,800	USD 13,800	USD 24,600	290.48%	7.00 meses
Favorable (+20%)	USD 12,960	USD 16,560	USD 29,520	368.57%	5.83 meses

Fuente: Elaboración propia.

Los resultados muestran que la propuesta mantiene un ROI positivo en los tres escenarios. En el escenario conservador, la inversión se recuperaría aproximadamente en 8.75 meses; en el escenario base, en siete meses; y en el escenario favorable, en 5.83 meses.

Sin embargo, la viabilidad financiera definitiva dependerá de la validación de las comisiones potencialmente preservadas, los reprocesos evitados y el costo real de la infraestructura. Por esta razón, los resultados deben interpretarse como proyecciones financieras referenciales y no como una garantía de ahorro.

6.7.13. COSTO DE OPORTUNIDAD DE NO IMPLEMENTAR EL MODELO

El costo de oportunidad de no implementar el modelo se relaciona con mantener una gestión informal, dispersa y limitada en trazabilidad. Esta condición puede generar demoras, atención repetitiva de incidencias, ausencia de evidencia documental y dificultades para priorizar los sistemas críticos.

Desde una perspectiva económica, la falta de un proceso formal mantiene la exposición a interrupciones en servicios comisionables. Las fallas en sistemas vinculados con ENEE, AMDC, AMSPS, matrícula vehicular, Hondutel y RAP pueden impedir temporalmente el procesamiento de operaciones o generar reprocesos adicionales.

En el ámbito regulatorio, la falta de registros centralizados puede dificultar la presentación de evidencia sobre las acciones realizadas, los responsables, los tiempos de atención y el cierre de las incidencias. Esto podría generar observaciones, requerimientos adicionales y mayor esfuerzo para reconstruir la información solicitada.

En los procesos internos, mantener información dispersa limita la generación de indicadores, dificulta la medición de los tiempos y reduce la visibilidad gerencial. Asimismo, aumenta el esfuerzo manual requerido para consolidar información y analizar el comportamiento de las incidencias.

Tabla 72. Costo de oportunidad de no implementar el modelo.

Condición si no se implementa	Consecuencia operativa	Posible impacto para Banco FICENSA
Registros informales o dispersos	Dificultad para reconstruir el historial de las incidencias	Menor trazabilidad y disponibilidad de evidencia
Reincidencias sin seguimiento estructurado	Repetición de incidencias en sistemas críticos	Mayor reproceso técnico y exposición a interrupciones
Interrupciones en servicios comisionables	Afectación de sistemas de pagos y recaudaciones	Posible pérdida de comisiones por operaciones no procesadas
Ausencia de SLA y alertas	Casos abiertos durante períodos prolongados	Incremento de los tiempos de resolución
Reportes manuales o dispersos	Mayor esfuerzo para consolidar información	Decisiones menos oportunas y menor visibilidad gerencial
Falta de cierre documentado	Casos sin validación final del usuario	Riesgo de soluciones incompletas o sin evidencia
Evidencia regulatoria insuficiente	Dificultad para demostrar la atención y el control de las incidencias	Mayor exposición a observaciones y requerimientos adicionales

Fuente: Elaboración propia.

La no implementación del modelo no representa necesariamente una pérdida económica inmediata y verificable. Sin embargo, conserva las condiciones que dificultan la trazabilidad, aumentan los reprocesos y limitan la capacidad institucional para controlar las incidencias de software.

6.7.14. VIABILIDAD FINANCIERA DE LA PROPUESTA

La propuesta presenta viabilidad financiera bajo los supuestos utilizados, debido a que aprovecha una plataforma existente y concentra la inversión incremental en el soporte especializado y la posible adquisición de infraestructura adicional.

La inversión incremental estimada asciende a USD 6,300. Los beneficios económicos se calculan únicamente a partir de las comisiones potencialmente preservadas y la reducción de reprocesos, excluyendo la monetización de sanciones y otros beneficios cualitativos.

En el escenario base, los beneficios ascienden a USD 10,800 durante el primer año y USD 13,800 durante el segundo. Esto representa un beneficio acumulado de USD 24,600 y un beneficio neto estimado de USD 18,300 al cierre del período analizado.

El ROI acumulado estimado es de 290.48% y el período de recuperación corresponde aproximadamente a siete meses. Estos resultados se explican porque el licenciamiento de

ServiceDesk Plus constituye un costo existente y no un desembolso adicional ocasionado por la propuesta.

El análisis de sensibilidad muestra resultados positivos en los escenarios conservador, base y favorable. No obstante, la viabilidad definitiva dependerá de validar las comisiones potencialmente preservadas, los reprocesos evitados y el costo real de la infraestructura.

Además de los resultados financieros, la propuesta genera beneficios cualitativos relacionados con la trazabilidad, el seguimiento, la medición de tiempos, la generación de reportes, la satisfacción del usuario y la disponibilidad de evidencia institucional.

En conclusión, el modelo representa una propuesta financieramente viable bajo los supuestos planteados. Sin embargo, los resultados deben interpretarse como estimaciones de planificación y no como beneficios garantizados, por lo que deberán actualizarse antes de la implementación con información validada por Banco FICENSA.

6.8. CONCORDANCIA DE LOS SEGMENTOS DE LA TESIS CON LA PROPUESTA

La propuesta desarrollada en el presente capítulo mantiene relación directa con los capítulos anteriores de la tesis. No surge como una solución aislada, sino como respuesta a la problemática identificada, al marco teórico desarrollado, a la metodología aplicada y a los resultados obtenidos durante el diagnóstico. Esta concordancia permite demostrar que el modelo propuesto responde de manera lógica a los hallazgos de la investigación y al objetivo general del estudio.

El Capítulo I permitió definir el problema central: la gestión de incidencias de software en las áreas de Negocios y Operaciones se realiza de forma parcialmente informal, sin un flujo completamente estructurado, lo que limita la trazabilidad, la medición de tiempos, el control de reincidencias y la generación de información confiable. A partir de este planteamiento, se definieron preguntas y objetivos orientados a analizar la situación actual y diseñar un modelo formal de gestión.

El Capítulo II aportó el sustento teórico de la propuesta, principalmente mediante ITIL 4, COBIT 2019, la Mesa de Servicio, los indicadores clave de desempeño, la gestión del riesgo tecnológico y la continuidad operativa. Estos elementos permitieron establecer que la gestión de

incidencias debe ser formal, trazable, medible y alineada con las necesidades del negocio. Además, el marco teórico permitió justificar el uso de ManageEngine ServiceDesk Plus como plataforma de apoyo para estructurar el flujo de atención.

El Capítulo III definió la metodología utilizada para analizar la situación actual. Mediante el enfoque cuantitativo, el cuestionario de percepción, la matriz documental de incidencias, la matriz de evaluación de capacidad basada en COBIT 2019 y los KPIs, se obtuvo información suficiente para construir una propuesta basada en evidencia. De esta forma, el modelo no depende únicamente de una opinión técnica, sino de datos recopilados y analizados durante la investigación.

El Capítulo IV presentó los resultados y hallazgos principales. En este capítulo se evidenciaron aspectos como la existencia de incidencias gestionadas sin registro formal, tiempos variables de atención y resolución, reincidencia de fallas, concentración de incidencias en determinadas áreas y sistemas, y una brecha de capacidad del proceso. Estos resultados sirvieron como base directa para definir los componentes del modelo: flujo formal, campos obligatorios, matriz de criticidad, SLA, reglas de escalamiento, matriz de responsabilidades e indicadores de seguimiento.

El Capítulo V integró las conclusiones y recomendaciones de la investigación. Estas recomendaciones funcionan como puente entre el diagnóstico y la propuesta, ya que orientan la necesidad de incorporar las incidencias de software dentro de un esquema formal, asignar responsables, medir el desempeño y fortalecer la trazabilidad del proceso. Por ello, el Capítulo VI convierte dichas recomendaciones en una propuesta aplicable para Banco FICENSA.

Tabla 73: Concordancia de los segmentos de la tesis con la propuesta

Segmento de la tesis	Aporte principal	Relación con la propuesta
Capítulo I. Planteamiento de la investigación	Define el problema, las preguntas de investigación, los objetivos y la justificación del estudio.	Justifica la necesidad de diseñar un modelo formal para gestionar las incidencias de software en Negocios y Operaciones.
Capítulo II. Marco teórico	Desarrolla los fundamentos de ITIL 4, COBIT 2019, Mesa de Servicio, KPIs, riesgo tecnológico y continuidad operativa.	Proporciona la base conceptual para estructurar el flujo, definir roles, establecer controles y medir el desempeño del proceso.
Capítulo III. Metodología	Define el enfoque, alcance, diseño, población, muestra, instrumentos, procedimientos y plan de análisis.	Permite demostrar que la propuesta se construye con base en información recopilada mediante instrumentos definidos y no únicamente por criterio subjetivo.

Segmento de la tesis	Aporte principal	Relación con la propuesta
Capítulo IV. Resultados y análisis	Presenta los resultados del cuestionario, matriz documental, evaluación de capacidad y KPIs.	Identifica las brechas que atiende la propuesta: informalidad, baja trazabilidad, tiempos variables, reincidencia y necesidad de medición.
Capítulo V. Conclusiones y recomendaciones	Sintetiza los hallazgos por objetivo y plantea acciones de mejora.	Sirve como base para convertir las recomendaciones en un modelo operativo aplicable dentro de la Mesa de Servicio existente.
Capítulo VI. Propuesta	Presenta el modelo formal de gestión de incidencias de software.	Integra el flujo de siete etapas, matriz de criticidad, SLA, responsables, KPIs, cronograma y presupuesto para su implementación.

Fuente: Elaboración propia.

La concordancia también puede observarse al relacionar cada objetivo específico con los componentes principales de la propuesta. Esto permite evidenciar que el modelo responde directamente a los propósitos de la investigación y que cada elemento propuesto tiene una razón de ser dentro del diagnóstico realizado.

Tabla 74: Concordancia entre objetivos específicos, hallazgos y componentes de la propuesta

Objetivo específico	Hallazgo relacionado	Componente de la propuesta que responde al hallazgo
Analizar la situación actual de la gestión de incidencias de software en las áreas de Negocios y Operaciones.	Se identificó una gestión parcialmente informal, con limitaciones de trazabilidad, control y seguimiento.	Formalización del proceso dentro de ManageEngine ServiceDesk Plus y definición de un flujo estructurado de siete etapas.
Calcular el tiempo promedio de atención y resolución de las incidencias de software.	Se evidenció la necesidad de medir y controlar los tiempos de atención y resolución.	Definición de SLA, tiempos objetivo y KPIs de atención y resolución.
Clasificar y cuantificar las incidencias de software según tipo, criticidad y área afectada.	Se identificó la necesidad de clasificar las incidencias para analizar patrones y priorizar la atención.	Campos obligatorios del ticket, categorías, subcategorías y matriz de criticidad basada en impacto y urgencia.
Determinar el porcentaje de incidencias de software gestionadas sin registro formal.	Se identificó una brecha de informalidad en el registro de incidencias.	Regla de uso del canal formal y obligación de convertir toda incidencia de software en ticket dentro de la Mesa de Servicio.
Establecer indicadores de desempeño para evaluar la gestión de incidencias de software del área de Desarrollo.	Se evidenció la necesidad de medir el desempeño mediante indicadores objetivos.	Tablero de KPIs: registro formal, tiempo de atención, tiempo de resolución, reincidencia, cumplimiento de SLA y cierre documentado.
Definir un flujo formal de registro, clasificación, escalamiento, seguimiento y cierre de incidencias de software.	La evaluación de capacidad mostró la necesidad de avanzar hacia un proceso más establecido, trazable y medible.	Modelo operativo de siete etapas, matriz de responsabilidades, reglas de escalamiento, validación del usuario y cierre formal.

Fuente: Elaboración propia.

En conjunto, la propuesta mantiene coherencia con el desarrollo completo de la tesis, debido a que transforma los hallazgos del diagnóstico en una solución concreta y aplicable. El modelo propuesto responde al problema planteado, utiliza los fundamentos teóricos desarrollados, se apoya en los datos obtenidos mediante la metodología y atiende las recomendaciones derivadas de los resultados. Por esta razón, el Capítulo VI representa la aplicación práctica de la investigación y la respuesta directa al objetivo general de diseñar un modelo de gestión de incidencias de software basado en ITIL 4 para Banco FICENSA.

7. BIBLIOGRAFÍA

- Al Wazzan, D. A. (14 de Abril de 2018). *A Framework for the Strategic Management of Information Technology*. American Journal of Business and Management: <https://doi.org/10.11634/216796061706918>
- Almendarez Rodríguez, V. H., & Cuéllar Varela, F. J. (2024). *Propuesta de optimización de la mesa de servicio para Banco Davivienda, alineada con las mejores prácticas de ITIL 4*. UNITEC.
- Anand, A. (6 de Enero de 2026). *ITIL 4 Explained: Framework, Practices, and Key Changes*. ITSM TOOLS: <https://itsm.tools/itil-4-explained/>
- AXELOS. (2019). *ITIL Foundation: ITIL 4 edition*. Londres: The Stationery Office.
- Ayala Soto, A. B., & Caso Rojas, C. A. (2023). *Implementación de las buenas prácticas de ITIL V4 y su influencia en la gestión de servicios del área de Service Desk de la empresa*. LIMA: Repositorio de la Universidad Autónoma del Perú.
- Banco Central de Honduras. (2023). *El Futuro del Dinero y los Pagos en Honduras. ¿Qué ruta seguir?* BCH.
- Banco Central de Honduras. (01 de Enero de 2026). *Vigilancia de los Sistemas de Pago*. www.bch.hn: <https://www.bch.hn/operativos/SP/Paginas/VIGILANCIA-DE-LOS-SISTEMA-DE-PAGO.aspx>
- Banco Ficensa. (2017). *Manual de Procesos Gestión de Tecnología*. Tegucigalpa: [Documento interno no publicado].
- Banco Ficensa. (2020). *Plan Estratégico de Tecnologías de Información y Comunicaciones 2020-2024*. Banco Ficensa. Tegucigalpa: [Documento interno no publicado].
- Banco Ficensa. (2024). *Acuerdos de nivel de servicio IT 2024*. Banco Ficensa, Tecnología. Tegucigalpa: [Documento interno no publicado].
- Basel Committee on Banking Supervision. (2011). *Principles for the sound management of operational risk*. Bank for International Settlements.
- Castro Martínez, L. Y., & Gómez Hernández, N. E. (2018). *Cambio de percepción de los colaboradores en la atención de tickets de TI de BAC Credomatic*. UNITEC.
- Comisión Nacional de Bancos y Seguros. (2022). *Circular CNBS No. 025-2022: Normas para la Gestión de Tecnologías de Información*. Tegucigalpa: Comisión Nacional de Bancos y Seguros. <https://circulares.cnbs.gob.hn/Archivo/Viewer/2520/025-2022%20NORMAS%20GESTION%20TECNOLOGIAS%20INFORMACION.pdf>
- Comisión Nacional de Bancos y Seguros. (2025). *La CNBS impulsa la inclusión e innovación financiera en el Fintech Day Honduras 2025*. <https://www.cnbs.gob.hn/inclusion-financiera/2025/10/14/la-cnbs-impulsa-la-inclusion-e-innovacion-financiera-en-el-fintech-day-honduras-2025/>
- Cots, S. (2011). *La estandarización de la gestión de TI a través de ISO/IEC 20.000*. Girona: Universitat de Girona.
- Deloitte. (29 de Junio de 2016). *¿Qué es el gobierno corporativo?* <https://www.deloitte.com/es/es/services/risk-advisory/perspectives/que-es-el-gobierno-corporativo.html>
- Downie, A., & O'Brien, K. (20 de Febrero de 2026). *¿Qué es la gobernanza de TI?* [ibm.com: https://www.ibm.com/think/topics/it-governance](https://www.ibm.com/think/topics/it-governance)

- Dzemydienė, D., Turskienė, S., & Šileikienė, I. (2024). *Un enfoque para la gestión de incidentes de TIC basado en las recomendaciones de la metodología ITIL 4*. Šiauliai, Lithuania: Baltic Journal of Modern Computing.
- El Herald. (31 de Marzo de 2024). *Fraude cibernético: ¿cómo lo combatirá el sector financiero?* El Herald: <https://www.elheraldo.hn/economia/fraude-cibernetico-combate-sector-financiero-honduras-NC12898511>
- Girsang, A. S., Kuncoro, Y., Saragih, M. H., & Nurul Fajar, A. (2018). *Implementación de un sistema de mesa de ayuda utilizando el framework ITIL en una empresa de software*. Computer Science Department. Jakarta: IOP Publishing Ltd. <https://doi.org/10.1088/1757-899X/420/1/012106>
- Gunawana, H., Pradipta Irianto, A. B., & Prima Negara, J. G. (14 de Abril de 2024). *Implementación de mejora sostenible del servicio en organizaciones utilizando el marco ITIL*. <https://doi.org/10.1016/j.procs.2024.03.061>
- Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. d. (2014). *Metodología de la investigación*. McGraw-Hill / Interamericana Editores, S.A. de C.V.
- IBM. (2006). *IT Service Management Standards*. IBM.
- IBM. (2023). *What is a service level agreement (SLA)?* IBM.
- IBM. (2023). *What is CSAT (Customer Satisfaction Score)?* IBM.
- IBM. (2023). *What is MTTR?* IBM. <https://www.ibm.com/es-es/think/topics/mttr>
- ISACA. (2018). *COBIT 2019*. ISACA.
- Jäntti, M., & Lindström, H. (6 de Enero de 2026). *Explorando los aspectos de calidad del autoservicio del cliente en la provisión de servicios de TI: un estudio de caso*. <https://doi.org/10.1016/j.jss.2025.112725>
- KnowledgeHut. (2023). *ITIL KPIs and metrics*. <https://www.knowledgehut.com/blog/it-service-management/itil-kpi>
- ManageEngine. (2024). *Guía definitiva de gestión de incidentes mayores*. <https://www.manageengine.com/latam/service-desk/itsm/guia-definitiva-gestion-de-incidentes-mayores.html>
- ManageEngine. (2024). *KPIs de gestión de incidentes de TI*. <https://www.manageengine.com/latam/service-desk/gestion-de-cambios-ti/kpis-de-gestion-de-incidentes-de-ti.html>
- MarketsandMarkets Research. (2025). *IT Service Management (ITSM) Market Size, Share & Forecast.*: <https://www.marketsandmarkets.com/Market-Reports/it-service-management-itsm-market-232882076.html>
- Marrone, M., Gacenga, F., Cater-Steel, A., & Kolbe, L. (31 de Marzo de 2014). *IT Service Management: A Cross-national Study of ITIL Adoption*. <https://doi.org/10.17705/1CAIS.03449>
- Martínez Dubón, E. D., & Andrade Suazo, J. F. (2021). *Diseño de un sistema de Service Desk basado en ITIL 4 y en las mejores prácticas de gestión de servicios en la Secretaría de Gobernación, Justicia y Descentralización*. UNITEC.
- Microsoft. (2023). *Build a cloud governance team*. <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/govern/build-cloud-governance-team>
- Moncada Martínez, A. V., & Godoy Godoy, E. M. (2025). *Propuesta de modelo para optimizar el proceso de adquisición de infraestructura tecnológica en la Universidad Nacional Autónoma de Honduras (UNAH), basado en COBIT 2019*. UNITEC.
- OGC. (2001). *ITIL V2*. Londres.

- OGC. (2011). *ITIL® Service Strategy*. Londres: The Stationery Office.
- Organización Internacional de Normalización. (2018). *ISO 31000:2018 Gestión del riesgo — Directrices*.
- Organización Internacional de Normalización. (2018). *ISO/IEC 20000-1 Sistema de gestión de servicios de TI*. Organización Internacional de Normalización.
<https://www.iso.org/standard/70636.html>
- Organización Internacional de Normalización. (2019). *ISO 22301: Sistemas de gestión de continuidad del negocio*.
- Petersen, K. (26 de Octubre de 2019). *Se necesita una comunidad de TI para desarrollar una mesa de servicio*. <https://doi.org/10.1145/3347709.3347832>
- Pujay Iglesias, I. L., & León, R. M. (2019). *Implementación de un modelo basado en ITIL para mejorar el proceso de atención de incidentes en el área de Help Desk de la empresa Contaperú*. LIMA: Repositorio de la Universidad Autónoma del Perú.
- Quiñónez Ku, V. X. (2018). *Implementación del proceso de gestión de incidencias basado en ITIL para mejorar la calidad del servicio del Departamento de TICS*. Universidad Católica del Ecuador. Universidad Católica del Ecuador.
- República de Honduras. (2004). *Ley del Sistema Financiero, Decreto No. 129-2004*. Congreso Nacional de la República.
- Rodríguez Archaga, W. J. (2024). *Propuesta de implementación de una mesa de servicio basada en las mejores prácticas de ITIL V4 para Industrias Pacer*. UNITEC.
- Sánchez Casanova, F. S. (15 de Agosto de 2021). *Implementación de ITIL versión 3 en las organizaciones: Razones del éxito y fracaso*.
<https://portal.amelica.org/ameli/jatsRepo/535/5352640006/index.html>
- Stuart D. Galup, R. D. (2009). *An Overview Of ITSM*. Commun. ACM.
<https://doi.org/10.1145/1506409.1506439>
- Tang, X., & Todo, Y. (2013). *Un estudio sobre la implementación de una mesa de servicio (Service Desk) en la gestión de servicios de TI en las empresas*. Kanazawa, Japón: Scientific Research Publishing. <https://doi.org/10.4236/ti.2013.43022>
- Virda Alfadina, A., Sulistiyani, E., & Nourma Budiarti, R. P. (2025). *Integración de ITIL V3, COBIT 5 y los estándares de Service Desk en el diseño de una mesa de servicio de TI*. Surabaya, Indonesia: ATCSI Journal – Applied Technology and Computing Science Journal. <https://journal2.unusa.ac.id/index.php/ATCSJ/article/download/8369/2984>
- White, S. K. (15 de Agosto de 2019). *What is ITSM? Managing IT to serve business needs*. ProQuest: <https://www.proquest.com/trade-journals/what-is-itsm-managing-serve-business-needs/docview/2273605975/se-2?accountid=35325>

8. ANEXOS

ANEXO 1: MATRIZ DE EVALUACIÓN DE CAPACIDAD DEL PROCESO BASADA EN COBIT 2019

El objetivo de este instrumento es evaluar el nivel de capacidad del proceso de gestión de incidencias de software en las áreas de Negocios y Operaciones del Banco Ficensa, conforme al modelo de evaluación de procesos de COBIT 2019.

Este instrumento será aplicado por el investigador con base en el análisis documental de las incidencias de software correspondientes al año 2025. Se deberá marcar el nivel que mejor represente la situación actual del proceso y documentar observaciones que sustenten la evaluación.

Tabla 75: Formato de Matriz de Evaluación de Capacidad del Proceso Basada en COBIT 2019

Nivel	Nombre del nivel	Descripción COBIT	Criterios de evaluación del proceso	Estado AS-IS	Estado TO-BE	Brecha	Observaciones
0	Incompleto	El proceso no logra su propósito	No existe gestión formal de incidencias, no hay registros ni control				
1	Ejecutado	El proceso logra su propósito de forma básica	Se atienden incidencias, pero sin documentación ni estandarización				
2	Gestionado	El proceso es planificado y supervisado	Existe control básico, seguimiento y cierta organización del proceso				

Nivel	Nombre del nivel	Descripción COBIT	Criterios de evaluación del proceso	Estado AS-IS	Estado TO-BE	Brecha	Observaciones
3	Establecido	El proceso está definido y estandarizado	Procedimientos documentados, roles definidos y flujo estructurado				
4	Predecible	El proceso es medido y controlado	Uso de indicadores, monitoreo del desempeño y control de tiempos				
5	Optimizado	El proceso se mejora continuamente	Mejora basada en métricas, análisis de tendencias e innovación del proceso				

Fuente: Elaboración Propia.

ANEXO 2: MATRIZ RA DEL PROCESO DE GESTIÓN DE INCIDENCIAS DE SOFTWARE

El presente instrumento tiene como objetivo definir y formalizar la asignación de roles y responsabilidades dentro del proceso propuesto de gestión de incidencias de software de Banco FICENSA, identificando quién ejecuta cada etapa del flujo y quién rinde cuentas por su resultado.

La matriz fue construida a partir del flujo formal de siete etapas desarrollado en el componente 6.4.2 del modelo, y respeta la estructura organizacional vigente de la Gerencia de Tecnología y Comunicaciones del banco. Su contenido se encuentra alineado con la práctica de Gestión de Incidencias definida por ITIL 4 (AXELOS, 2019) y con los principios de gobierno establecidos por COBIT 2019 a través del objetivo de gestión DSS02 (ISACA, 2018).

Se deberá asignar una letra según el nivel de participación de cada rol en cada actividad:

R = Responsable: rol encargado de ejecutar directamente la actividad.

A = Accountable: rol que rinde cuentas por el resultado de la actividad, valida su

cumplimiento y asume la responsabilidad final.

Cuando un rol comparte ejecución bajo condiciones diferenciadas, se indica con notas al pie. Cuando ningún rol participa, la celda queda en blanco

Roles considerados:

#	Rol	Abreviatura
1	Colaborador reportante de Negocios u Operaciones	Colaborador
2	Oficial de Soporte Proyectos / Help Desk	Oficial HD
3	Oficial de Soporte Cash Management	Oficial CM
4	Analista Programador Senior	Analista Sr
5	Analistas Programadores Junior	Analista Jr
6	Jefe de Proyectos y Desarrollo	Jefe PyD
7	Gerente de Tecnología y Comunicaciones	Gerente TIC

Tabla 76: Formato de Matriz RA del Proceso de Gestión de Incidencias

Actividad del proceso	Colaborador	Oficial HD	Oficial CM	Analista Sr	Analista Jr	Jefe PyD	Gerente TI
Etapas 1 -Registro							
Etapas 2 – Validación							
Etapas 3 – Clasificación							
Etapas 4 – Priorización							
Etapas 5 – Asignación							
Etapas 6 – Diagnostico y Resolución.							
Etapas 7 – Validación del usuario y cierre formal							

Fuente: Elaboración Propia.

ANEXO 3: MATRIZ DE INDICADORES CLAVE DE DESEMPEÑO (KPIs)

El objetivo del instrumento es medir y monitorear el desempeño del proceso de gestión de incidencias de software mediante indicadores cuantitativos relacionados con la trazabilidad, la oportunidad de atención, la eficiencia de resolución y la reincidencia de las fallas.

La matriz distingue dos momentos de medición. En primer lugar, se establecen cuatro indicadores que permiten construir la línea base del proceso actual a partir de la base de datos consolidada de incidencias correspondiente al año 2025, obtenida mediante la revisión de correos electrónicos, reportes internos y registros disponibles. En segundo lugar, se incorporan dos indicadores de seguimiento futuro, los cuales deberán medirse una vez que las incidencias de software sean integradas formalmente dentro de la Mesa de Servicio institucional y se implemente el flujo propuesto.

Los resultados obtenidos permitirán comparar el estado actual del proceso con su evolución posterior, identificar brechas, analizar tendencias y orientar acciones de mejora continua.

Tabla 77: Formato de matriz de indicadores clave de desempeño (KPIs)

KPI	Momento de aplicación	Definición	Fórmula	Fuente de datos	Frecuencia	Observaciones
Porcentaje de incidencias gestionadas sin registro formal	Línea base 2025 y seguimiento o futuro	Proporción de incidencias atendidas mediante canales no formalizados respecto al total de casos identificados.	$\left(\frac{\text{Incidencias sin registro formal}}{\text{Total de incidencias identificadas}} \right) \times 100$	Base consolidada de incidencias y registros de Mesa de Servicio	Mensual	
Tiempo promedio de atención	Línea base 2025 y seguimiento o futuro	Promedio del tiempo transcurrido entre el reporte inicial de la	$\frac{\text{Suma de tiempos de atención}}{\text{Total de incidencias con fecha}}$	Base consolidada de incidencias y registros	Mensual	

		incidencia y el inicio documentado de su atención.	de reporte y fecha de atención verificables	de Mesa de Servicio		
Tiempo promedio de resolución de incidencias (MTTR, Mean Time to Resolution)	Línea base 2025 y seguimiento o futuro	Promedio del tiempo transcurrido entre el reporte inicial de la incidencia y su solución documentada.	Suma de tiempos de resolución / Total de incidencias resueltas con datos completos	Base consolidada de incidencias y registros de Mesa de Servicio	Mensual	
Tasa de reincidencia	Línea base 2025 y seguimiento o futuro	Proporción de incidencias que se repiten en el mismo sistema, módulo o proceso respecto al total de casos identificados.	(Incidencias reinincidentes / Total de incidencias identificadas) $\times$ 100	Base consolidada de incidencias y registros de Mesa de Servicio	Mensual	
Cumplimiento de acuerdos de nivel de servicio (SLA)	Seguimiento o futuro	Proporción de incidencias atendidas y resueltas dentro de los tiempos definidos según su nivel de criticidad.	(Incidencias gestionadas dentro del SLA / Total de incidencias evaluadas) $\times$ 100	Registros de Mesa de Servicio y acuerdos de nivel de servicio definidos	Mensual	Su medición iniciará después de formalizar los SLA aplicables a incidencias de software.

Porcentaje de incidencias con trazabilidad completa	Seguimiento o futuro	Proporción de incidencias que cuentan con registro formal, clasificación, prioridad, responsable asignado, evidencia de seguimiento, solución documentada y confirmación de cierre.	(Incidencias con trazabilidad completa / Total de incidencias registradas) × 100	Registros de Mesa de Servicio	Mensual	Su medición iniciará después de implementar el flujo formal propuesto.
--	----------------------	---	--	-------------------------------	---------	--

Fuente: Elaboración Propia.

ANEXO 4: CUESTIONARIO DE PERCEPCIÓN DEL USUARIO

El presente cuestionario constituye el instrumento principal utilizado para la recolección, medición y análisis de la experiencia de los usuarios finales frente al modelo actual de soporte técnico de Banco Ficensa ante las incidencias de Software. Este instrumento fue diseñado en formato digital estructurado con el propósito de cuantificar la opinión del censo de colaboradores pertenecientes a usuarios del software interno del banco, permitiendo transformar percepciones subjetivas en datos estadísticos rígidamente medibles.

El instrumento incorpora dimensiones específicas estructuradas bajo la escala de Likert que facilitan la evaluación de la satisfacción general, la percepción sobre los tiempos de respuesta, la claridad en el seguimiento de los casos y los efectos operativos derivados de la existencia de múltiples canales de reporte no estandarizados.

Enlace a encuesta digital: [Encuesta sobre la Percepción de la Gestión de Incidencias de Software en Banco Ficensa: Rellenar formulario](#)

Encuesta sobre la Percepción de la Gestión de Incidencias de Software en Banco Ficensa

Estimado colaborador: El presente cuestionario tiene como propósito recopilar información sobre su experiencia actual al reportar fallas o incidencias de software al departamento de Tecnologías de la Información (TI). Su participación es fundamental para el desarrollo de un Trabajo Final de Graduación de Maestría en UNITEC. Sus respuestas serán tratadas de manera estrictamente anónima, confidencial y consolidada con fines puramente estadísticos. El tiempo estimado para completarlo es de 5 a 10 minutos. ¡Muchas gracias por su colaboración!

Cuando envíe este formulario, no recopilará automáticamente sus detalles, como el nombre y la dirección de correo electrónico, a menos que lo proporcione usted mismo.

* Obligatorio

Sección I. Datos de identificación

1. Área a la que pertenece *

Selecciona la respuesta ▼

2. Antigüedad en Banco Ficensa *

☐ Menos de 1 año

☐ De 1 a 3 años

☐ De 3 a 5 años

☐ Más de 5 años

Siguiendo

Figura 38: Cuestionario Utilizado en Recolección de Datos

Fuente: Elaboración propia

Estructura del instrumento

El cuestionario se organizó en tres secciones. La Sección I recolectó información sociodemográfica; la Sección II, los hábitos de reporte actuales; y la Sección III, la evaluación de percepción y satisfacción mediante escala de Likert de cinco niveles (1 = Totalmente en desacuerdo; 2 = En desacuerdo; 3 = Ni de acuerdo ni en desacuerdo; 4 = De acuerdo; 5 = Totalmente de acuerdo).

Ítems que integran la escala de confiabilidad

Para el cálculo del coeficiente Alfa de Cronbach ($\alpha = 0.807$) se consideraron los quince ítems orientados a valorar la percepción sobre la calidad del servicio actual y la disposición hacia un modelo centralizado, correspondientes a las preguntas 9, 10, 11, 13, 21, 22, 23, 24, 26, 27, 28, 29, 30, 31 y 32 del presente instrumento. Los ítems restantes de la Sección III, de carácter diagnóstico sobre hábitos y dificultades del proceso, se analizaron de forma descriptiva e independiente en el Capítulo IV.

ANEXO 5: FORMATO MATRIZ DOCUMENTAL DE INCIDENTES DE SOFTWARE

La presente matriz de recolección de datos documentales constituye el instrumento utilizado para el registro, organización y sistematización de las incidencias de software correspondientes al año 2025.

Esta matriz fue diseñada en formato de base de datos con el propósito de consolidar la información proveniente de diversas fuentes documentales, tales como correos electrónicos, llamadas telefónicas y Teams, permitiendo estructurar datos que originalmente se encontraban dispersos y sin un esquema formal de registro.

El instrumento incorpora campos específicos que facilitan la clasificación de las incidencias según fecha de reporte, área afectada, sistema involucrado, tipo de incidencia, medio de registro, tiempos de atención y resolución, nivel de criticidad y reincidencia.

Tabla 78: Formato Matriz Documental de Incidentes de Software

ID	Fecha Reporte	Área	Sistema	Tipo	Descripción	Medio	Fecha Atención	Fecha Resolución	Tiempo de Atención	Tiempo de Resolución	Criticidad	Estado	Reincidencia

Fuente: Elaboración Propia.

ANEXO 6: MATRIZ DOCUMENTAL DE INCIDENTES DE SOFTWARE CONSOLIDADA CON LAS INCIDENCIAS REGISTRADAS DURANTE EL AÑO 2025.

A continuación, se presenta la síntesis de matriz documental de incidencias, en la cual se consolidan todas las incidencias de software recopiladas durante el año 2025.

Tabla 79: Síntesis de la matriz documental de incidencias de software, año 2025.

Grupo	Fecha de reporte	Área	Sistema	Tipo	Descripción resumida	Medio	Fecha de atención	Fecha de resolución	Tiempo de atención	Tiempo de resolución	Criticidad	Estado	Reincidencia	Tipo de registro	Cantidad de incidencias	Porcentaje sobre el total
1	01/01/2025 - 01/12/2025	Negocios	Inclusión Financiera	Falla funcional	Error recurrente en generación de reporte CNBS por inconvenientes de software y base de datos; se recurrió a ambiente de pruebas como medida temporal.	Correo	01/01/2025 - 01/12/2025	Sin dato	Prom. 0.00 días	N/A	Media	Sin resolver	Sí	Formal	12	21.43%
2	02/06/2025 - 21/11/2025	Operaciones	ENEE	Falla funcional, integración y datos incorrectos	Errores de comunicación con ente externo, caracteres especiales en débitos automáticos, problemas de conexión, reversas y formato de claves.	Correo, Teams y WhatsApp	02/06/2025 - 21/11/2025	02/07/2025 - 22/11/2025	Prom. 2.78 días	Prom. 7.56 días	Media y baja	Resuelto	Sí / No	Formal e informal	9	16.07%
3	02/06/2025 - 22/12/2025	Operaciones	Alcaldía Municipal del Distrito Central / AMDC	Integración y datos incorrectos	Problemas de comunicación con proveedor externo, errores timeout, cambios de campos obligatorios y consultas con información incorrecta.	Teams, WhatsApp y Correo	02/06/2025 - 22/12/2025	02/07/2025 - 23/12/2025	Prom. 1.40 días	Prom. 16.60 días	Baja, media y alta	Resuelto	Sí / No	Formal e informal	5	8.93%

4	02/06/2025 - 17/10/2025	Operaciones	RAP	Integración	Inconsistencias en comunicación con servicio RAP, timeout y transacciones registradas del lado del proveedor sin reflejarse internamente.	Teams	02/06/2025 - 17/10/2025	02/06/2025 - 18/10/2025	Prom. 0.00 días	Prom. 0.50 días	Media y alta	Resuelto	Sí	Informal	2	3.57%
5	15/08/2025 - 18/08/2025	Operaciones	Conciliación SINAP	Integración	Errores timeout durante cierre de débito y proceso de conciliación SINAP.	Teams	19/8/2025	20/8/2025	Prom. 2.50 días	Prom. 3.50 días	Media	Resuelto	Sí	Informal	2	3.57%
6	03/03/2025 - 12/09/2025	Operaciones	Matrícula Vehicular	Integración y falla funcional	Errores por formato de boletas, ceros a la izquierda y diferencias entre ambiente de pruebas y producción.	Correo	03/03/2025 - 12/09/2025	09/03/2025 - 08/10/2025	Prom. 0.00 días	Prom. 16.00 días	Alta y media	Resuelto	No	Formal	2	3.57%
7	17/4/2025	Operaciones	ACH	Integración	Incidencia relacionada con usuario maestro ACH.	Teams	20/4/2025	Sin dato	3 días	N/A	Alta	Sin resolver	No	Informal	1	1.79%
8	18/1/2025	Operaciones	ACH- Participantes Indirectos	Integración	Incidencia registrada en fase de cierre relacionada con ACH- Participantes Indirectos.	Teams	19/1/2025	25/1/2025	1 día	7 días	Baja	Resuelto	No	Informal	1	1.79%
9	15/4/2025	Negocios	App	Falla funcional	Incidencia relacionada con versión de aplicación en fase de planeación.	Teams	19/4/2025	Sin dato	4 días	N/A	Media	Sin resolver	No	Informal	1	1.79%
10	26/5/2025	Operaciones	BALCAM	Falla funcional	Incidencia en bandeja de aprobaciones.	Teams	27/5/2025	Sin dato	1 día	N/A	Alta	Sin resolver	No	Informal	1	1.79%

11	5/5/2025	Negocios	CIC	Falla funcional	Incidencia asociada a mejoras del sistema CIC.	Teams	6/5/2025	Sin dato	1 día	N/A	Media	Sin resolver	No	Informal	1	1.79%
12	4/6/2025	Operaciones	CREFISA	Falla funcional	Incidencia relacionada con pago de préstamo.	Teams	4/6/2025	Sin dato	0 días	N/A	Media	Sin resolver	No	Informal	1	1.79%
13	23/3/2025	Operaciones	Campo DNI largo excedido	Error	Error asociado a longitud excedida del campo DNI.	Teams	26/3/2025	29/3/2025	3 días	6 días	Baja	Resuelto	No	Informal	1	1.79%
14	4/7/2025	Negocios	DATAPRO	Falla funcional	Incidencia relacionada con mesa de ayuda DATAPRO.	Teams	6/7/2025	Sin dato	2 días	N/A	Media	Sin resolver	No	Informal	1	1.79%
15	24/1/2025	Negocios	DEVINC	Falla funcional	Incidencia registrada en fase de planeación.	Teams	27/1/2025	Sin dato	3 días	N/A	Media	Sin resolver	No	Informal	1	1.79%
16	4/9/2025	Negocios	Doble Factor Autenticación	Falla funcional	Incidencia relacionada con doble factor de autenticación.	Teams	7/9/2025	8/9/2025	3 días	4 días	Baja	Resuelto	No	Informal	1	1.79%
17	20/6/2025	Operaciones	Débito automático	Falla funcional	Incidencia 500 en proceso de débito automático.	Teams	22/6/2025	Sin dato	2 días	N/A	Alta	Sin resolver	No	Informal	1	1.79%
18	28/7/2025	Operaciones	Devolución 8%	Error	Cambio de formato de archivo XLS a XLSX sin notificación previa, generando incompatibilidad en procesamiento.	Correo	29/7/2025	31/7/2025	1 día	3 días	Alta	Resuelto	No	Formal	1	1.79%
19	19/6/2025	Operaciones	Firmas	Falla funcional	Incidencia relacionada con migración de autobancos.	Teams	20/6/2025	26/6/2025	1 día	7 días	Baja	Resuelto	No	Informal	1	1.79%
20	25/4/2025	Negocios	Hondutel	Falla funcional	Incidencia de usuario relacionada con Hondutel.	Teams	27/4/2025	Sin dato	2 días	N/A	Media	Sin resolver	No	Informal	1	1.79%

21	28/2/2025	Operaciones	Levantamiento Metas-Mejoras RRHH	Falla funcional	Incidencia relacionada con levantamiento de metas y mejoras de RRHH.	Teams	1/3/2025	8/3/2025	1 día	8 días	Baja	Resuelto	No	Informal	1	1.79%
22	9/11/2025	Operaciones	MT940	Falla funcional	Incidencia CRUD relacionada con MT940.	Teams	14/11/2025	Sin dato	5 días	N/A	Media	Sin resolver	No	Informal	1	1.79%
23	12/3/2025	Operaciones	Módulo Proveeduría	Falla funcional	Incidencia relacionada con módulo de Proveeduría.	Teams	14/3/2025	16/3/2025	2 días	4 días	Baja	Resuelto	No	Informal	1	1.79%
24	21/8/2025	Operaciones	Módulo administrativo	Falla funcional	Incidencia relacionada con actualización del módulo administrativo.	Teams	23/8/2025	Sin dato	2 días	N/A	Media	Sin resolver	No	Informal	1	1.79%
25	21/11/2025	Negocios	Notificaciones	Falla funcional	Incidencia relacionada con llave duplicada en sistema de notificaciones.	Teams	21/11/2025	Sin dato	0 días	N/A	Media	Sin resolver	No	Informal	1	1.79%
26	21/10/2025	Negocios	RCL	Falla funcional	Incidencia registrada en fase de ajustes.	Teams	22/10/2025	Sin dato	1 día	N/A	Alta	Sin resolver	No	Informal	1	1.79%
27	15/3/2025	Operaciones	REDESA	Falla funcional	Incidencia relacionada con reserva de sala.	Teams	18/3/2025	Sin dato	3 días	N/A	Media	Sin resolver	No	Informal	1	1.79%
28	24/9/2025	Operaciones	ReclamosCNBS	Falla funcional	Incidencia relacionada con código de respuesta.	Teams	25/9/2025	Sin dato	1 día	N/A	Media	Sin resolver	No	Informal	1	1.79%
29	21/5/2025	Operaciones	SIISAR	Falla funcional	Incidencia registrada en fase de cierre.	Teams	26/5/2025	31/5/2025	5 días	10 días	Baja	Resuelto	No	Informal	1	1.79%
30	22/4/2025	Operaciones	TSP	Falla funcional	Incidencia registrada en fase de planeación.	Teams	24/4/2025	Sin dato	2 días	N/A	Media	Sin resolver	No	Informal	1	1.79%

Fuente: Elaboración Propia.

ANEXO 7: POLÍTICA INSTITUCIONAL DE GESTIÓN DE INCIDENCIAS DE SOFTWARE — BANCO FICENSA

Código:	BF-GTI-POL.PYD.001-1.0.0
Clasificación:	Interno
Gerencia:	Gerencia de Tecnología y Comunicaciones
Fecha de emisión:	__/__/____
Elaborado por:	Ronaldo Enrrique Cárcamo Vásquez y Alex Gerardo Gámez Arteaga
Revisado por:	Jefe de Proyectos y Desarrollo
Aprobado por:	Gerente de Tecnología y Comunicaciones

INTRODUCCIÓN

La gestión de las incidencias de software constituye un proceso crítico para el desempeño operativo del sector bancario, dado que su correcta administración influye directamente en la continuidad del servicio, la satisfacción del cliente interno y el control del riesgo tecnológico. En el contexto actual de Banco FICENSA, las áreas de Negocios y Operaciones presentan una alta dependencia de los sistemas de software para el cumplimiento de sus funciones, situación que demanda contar con un instrumento normativo capaz de regular de manera uniforme el tratamiento institucional de las incidencias.

El presente documento establece la Política Institucional de Gestión de Incidencias de Software de Banco FICENSA, formulada con base en las mejores prácticas internacionales contenidas en el marco ITIL 4 y en los lineamientos de gobierno establecidos por COBIT 2019. Su contenido fue desarrollado a partir del diagnóstico de la situación actual del proceso, identificando las brechas operativas que justifican la formalización de criterios institucionales para el registro, atención, resolución y cierre de los casos.

La política tiene como propósito esencial garantizar la trazabilidad completa del ciclo de vida de cada incidencia, asegurar tiempos de respuesta proporcionales al impacto operativo y fortalecer la capacidad institucional para prevenir la recurrencia de fallas en los sistemas críticos del banco. Su aplicación es de carácter obligatorio para todos los colaboradores de las áreas de Negocios y Operaciones, así como para el personal técnico responsable de la atención y resolución de las incidencias dentro de la Gerencia de Tecnología y Comunicaciones.

DISPOSICIONES GENERALES

ÁMBITO DE APLICACIÓN

La presente política aplica a todas las áreas funcionales de Banco FICENSA cuyas operaciones se desarrollan total o parcialmente mediante el uso de sistemas de software, de manera particular a las áreas de Negocios y Operaciones y a las unidades organizacionales que de ellas dependen. Su cumplimiento es de carácter obligatorio y se materializa mediante la plataforma institucional ManageEngine ServiceDesk Plus, designada como canal único de registro, gestión y trazabilidad de las incidencias.

OBJETIVO NORMATIVO

La política responde a la necesidad institucional de estandarizar el tratamiento de las incidencias de software, eliminar la dispersión de canales y garantizar el control documental del proceso. Su finalidad estructural consiste en establecer un marco normativo único que permita a Banco FICENSA elevar la capacidad del proceso conforme a los niveles establecidos por el modelo COBIT 2019 y cumplir con los requerimientos regulatorios aplicables al sistema financiero nacional.

PRINCIPIOS ORIENTADORES

La aplicación de la política se orienta por los principios institucionales de trazabilidad, oportunidad, responsabilidad, mejora continua y orientación al servicio. Estos principios son coherentes con los valores corporativos de Banco FICENSA y con la cultura de gobierno tecnológico que la institución promueve en cumplimiento de su Plan Estratégico de Tecnologías de Información y Comunicaciones.

RESPONSABILIDAD COMPARTIDA

El cumplimiento de la política es una responsabilidad compartida entre los colaboradores reportantes, el personal de soporte de primer nivel, el segundo nivel técnico y las jefaturas funcionales. Cada nivel asume responsabilidades específicas dentro del ciclo de vida de la incidencia, conforme a lo establecido en el numeral 5.2 del presente documento.

REVISIÓN Y MEJORA

Las disposiciones aquí descritas podrán ser actualizadas conforme a los procesos de la Gerencia de Tecnología y Comunicaciones, Gestión de Calidad, Auditoría Interna o necesidades operativas detectadas durante la aplicación cotidiana del modelo, previa validación del área encargada de la gestión documental del banco.

1. OBJETIVO

Establecer las reglas institucionales que rigen el reporte, registro, atención, resolución y cierre formal de las incidencias de software que afectan la operación de las áreas de Negocios y Operaciones de Banco FICENSA, con el propósito de garantizar la trazabilidad completa del ciclo de vida de cada caso, asegurar tiempos de respuesta proporcionales al impacto operativo y fortalecer la capacidad institucional para prevenir su recurrencia.

2. ALCANCE

La presente política aplica a todos los colaboradores de las áreas de Negocios y Operaciones de Banco FICENSA, en cualquiera de las unidades organizacionales que las conforman, responsables de reportar incidencias relacionadas con los sistemas de software utilizados para la operación bancaria.

Asimismo, aplica al personal técnico de la Gerencia de Tecnología y Comunicaciones responsable de la atención, diagnóstico, resolución y cierre de las incidencias reportadas, así como a las jefaturas de Negocios y Operaciones encargadas de promover su cumplimiento dentro de sus respectivos equipos.

Quedan excluidas del alcance las incidencias relacionadas con hardware, infraestructura de redes, telecomunicaciones, seguridad física y eventos asociados a la gestión de capacidad de la plataforma tecnológica, las cuales se rigen por instrumentos normativos específicos y son atendidas por el área de Infraestructura, Redes y Comunicaciones.

3. MARCO LEGAL Y NORMATIVO

La presente política se sustenta en la siguiente normativa nacional e internacional, así como en los estándares metodológicos que orientan las mejores prácticas en gestión de servicios de tecnología de información.

No.	Tipo	Código	Nombre
1	Resolución	CNBS No. 025-2022	Resolución sobre lineamientos para la gestión de la tecnología de información y comunicaciones de las instituciones del sistema financiero.
2	Decreto Legislativo	Decreto No. 129-2004	Ley del Sistema Financiero de Honduras.
3	Estándar Internacional	ITIL 4	Marco de referencia para la gestión de servicios de tecnología de información, publicado por AXELOS.
4	Estándar Internacional	COBIT 2019	Marco de referencia para el gobierno y la gestión de la información y la tecnología empresarial, publicado por ISACA.
5	Norma Internacional	ISO/IEC 20000-1:2018	Tecnología de la Información — Gestión de Servicios — Parte 1: Requisitos del sistema de

No.	Tipo	Código	Nombre
			gestión de servicios.
6	Documento Institucional	PETI FICENSA 2020	Plan Estratégico de Tecnologías de Información y Comunicaciones de Banco FICENSA.

4. DEFINICIONES

Para efectos de la presente política, los términos enlistados a continuación tendrán el significado que se indica.

- **Acuerdo de Nivel de Servicio (SLA):** compromiso documentado entre el proveedor del servicio y el usuario, que establece los tiempos máximos para la atención inicial, diagnóstico, resolución, validación y cierre formal de una incidencia, en función de su nivel de criticidad.
- **Canal único de gestión:** plataforma institucional designada para el registro consolidado de toda incidencia de software, identificada como ManageEngine ServiceDesk Plus, con independencia del canal por el cual el usuario realice el reporte inicial.
- **Ciclo de vida de la incidencia:** secuencia ordenada de etapas por las cuales atraviesa una incidencia desde su reporte por parte del usuario hasta su cierre formal documentado en la plataforma.
- **Cierre formal:** estado final del ticket en el cual la incidencia ha sido resuelta, validada por el usuario reportante y debidamente documentada, conforme al procedimiento institucional aplicable.
- **Escalamiento:** mecanismo formal por el cual una incidencia es trasladada a un nivel técnico superior cuando excede los tiempos definidos por el acuerdo de nivel de servicio o cuando supera la capacidad técnica del nivel actual de atención.
- **Incidencia:** interrupción no planificada o degradación de la calidad de un servicio de software que afecta la operación normal de las áreas de Negocios u Operaciones de Banco FICENSA.
- **ManageEngine ServiceDesk Plus:** plataforma tecnológica institucional designada por Banco FICENSA como herramienta única para la gestión, trazabilidad y documentación de las incidencias de software.
- **Mesa de Servicio:** función organizacional ejercida por el Oficial de Soporte Proyectos / Help Desk y el Oficial de Soporte Cash Management, responsable del registro, validación, clasificación, priorización y asignación de las incidencias en su primer nivel de atención.
- **Reincidencia:** ocurrencia repetida de una incidencia con el mismo origen funcional, sistema

afectado o causa raíz, dentro de un periodo definido por la institución.

- **Registro formal:** creación de un ticket dentro de la plataforma ManageEngine ServiceDesk Plus, con la totalidad de los campos obligatorios completados conforme al procedimiento institucional vigente.
- **Trazabilidad:** propiedad del proceso que permite reconstruir, en cualquier momento, la secuencia completa de eventos, decisiones y actores involucrados en la atención de una incidencia desde su reporte hasta su cierre.

5. LINEAMIENTOS PARA LA GESTIÓN DE INCIDENCIAS DE SOFTWARE

Los presentes lineamientos rigen la actuación de todos los actores involucrados en el proceso de gestión de incidencias de software dentro de Banco FICENSA. Su aplicación es obligatoria y se desarrolla en tres niveles: lineamientos generales, asignación de roles y responsabilidades, y gestión operativa del modelo.

5.1 Lineamientos Generales

5.1.1 Toda incidencia de software que afecte la operación de las áreas de Negocios y Operaciones de Banco FICENSA deberá ser registrada formalmente en la plataforma ManageEngine ServiceDesk Plus, dentro del tiempo definido por el acuerdo de nivel de servicio aplicable a su nivel de criticidad.

- a. El registro formal será obligatorio con independencia del canal por el cual el usuario haya efectuado el reporte inicial, incluyendo correo electrónico, mensajería corporativa, llamada telefónica o comunicación presencial.
- b. Ningún caso deberá atenderse, resolverse o cerrarse fuera de la plataforma institucional designada.
- c. La omisión del registro formal constituirá un incumplimiento de la presente política y será tratada conforme a los mecanismos internos de control del banco.

5.1.2 El Oficial de Soporte Proyectos / Help Desk será responsable de garantizar la creación del registro institucional ante cualquier comunicación recibida por canales no oficiales, asegurando la documentación uniforme de la totalidad de las incidencias.

- a. Cuando el reporte inicial corresponda al sistema Cash Management, esta responsabilidad recaerá en el Oficial de Soporte Cash Management dentro de su ámbito de especialización.

5.1.3 Toda incidencia registrada deberá contar con clasificación, priorización y asignación formal antes de su escalamiento al segundo nivel técnico, conforme a la matriz de criticidad

institucional.

5.1.4 La trazabilidad completa del ciclo de vida de la incidencia deberá quedar documentada en la plataforma, incluyendo el diagnóstico técnico, las acciones de resolución, la validación por parte del usuario y el cierre formal del caso.

5.1.5 Las incidencias clasificadas como reincidentes en un mismo sistema o módulo, dentro del periodo definido institucionalmente, deberán ser escaladas a la práctica de Gestión de Problemas para su correspondiente análisis de causa raíz.

5.2 Roles y Responsabilidades

La presente política asigna las siguientes funciones específicas a cada actor involucrado en el proceso de gestión de incidencias de software.

Gerencia de Tecnología y Comunicaciones:

- a. Aprobar, mantener vigente y actualizar la presente política.
- b. Autorizar excepciones formales al cumplimiento de la política.
- c. Supervisar los indicadores clave de desempeño del proceso.

Jefe de Proyectos y Desarrollo:

- a. Coordinar tácticamente la operación del modelo dentro de su línea de mando.
- b. Garantizar el cumplimiento de los acuerdos de nivel de servicio.
- c. Asignar y supervisar los recursos del segundo nivel técnico.
- d. Validar el cierre técnico de las incidencias críticas.

Oficial de Soporte Proyectos / Help Desk:

- a. Ejercer la función de Mesa de Servicio como primer nivel de atención.
- b. Registrar, validar, clasificar, priorizar y asignar cada incidencia recibida.
- c. Garantizar el registro formal de los reportes recibidos por canales no oficiales.
- d. Documentar las acciones realizadas durante el primer nivel de atención.

Oficial de Soporte Cash Management:

- a. Cumplir las funciones del primer nivel de atención para las incidencias específicas del sistema Cash Management.
- b. Coordinar con el Oficial de Soporte Proyectos / Help Desk los casos que requieran articulación con otros sistemas.

Analista Programador Senior y Analistas Programador Junior:

- a. Realizar el diagnóstico, la resolución y la documentación técnica de los casos escalados al segundo nivel.
- b. Aplicar las soluciones bajo los tiempos establecidos en el acuerdo de nivel de servicio.
- c. Notificar al primer nivel la resolución del caso para su validación con el usuario.

Jefaturas de las áreas de Negocios y Operaciones:

- a. Promover la adopción de la política entre los colaboradores de su área.
- b. Validar la solución brindada antes del cierre formal del caso.
- c. Reportar a la Gerencia de Tecnología y Comunicaciones los incumplimientos que detecten.

Colaboradores reportantes:

- a. Reportar oportunamente las incidencias de software detectadas durante el desarrollo de sus funciones.
- b. Proporcionar la información requerida para el registro formal del caso.
- c. Validar la solución brindada antes del cierre formal.

5.3 Gestión Operativa del Modelo

5.3.1 El proceso de atención de incidencias se ejecutará conforme al flujo formal de siete etapas establecido por el modelo institucional: registro, validación, clasificación, priorización, asignación, diagnóstico y resolución, y validación y cierre.

5.3.2 La priorización de las incidencias se realizará conforme a la matriz de criticidad institucional, considerando el impacto operativo del caso y la importancia estratégica del sistema afectado.

5.3.3 Los acuerdos de nivel de servicio aplicables a cada nivel de criticidad serán supervisados de manera automatizada por la plataforma, con alertas tempranas ante riesgo de incumplimiento.

5.3.4 El desempeño del proceso será medido conforme a los seis indicadores clave de desempeño institucionalizados por el modelo, los cuales serán reportados periódicamente a la Gerencia de Tecnología y Comunicaciones.

6. DISPOSICIONES FINALES

6.1 La presente política entrará en vigencia a partir de la fecha de su aprobación formal por parte de la Gerencia de Tecnología y Comunicaciones de Banco FICENSA y permanecerá vigente hasta que sea modificada o derogada mediante un nuevo instrumento normativo

emitido por la misma autoridad.

6.2 La política será revisada de manera ordinaria con periodicidad anual y de manera extraordinaria cuando se identifiquen cambios regulatorios, organizacionales o tecnológicos que justifiquen su actualización.

6.3 Toda excepción al cumplimiento de la política deberá ser solicitada formalmente ante la Gerencia de Tecnología y Comunicaciones, justificada por escrito y autorizada de manera expresa. Ninguna excepción operará de manera automática ni podrá invocarse de forma retroactiva.

6.4 La interpretación oficial del contenido de la presente política corresponde a la Gerencia de Tecnología y Comunicaciones, quien resolverá las dudas que surjan durante su aplicación cotidiana.

6.5 Los anexos del presente documento forman parte integral del mismo y su contenido es de cumplimiento obligatorio para todos los actores involucrados.

7. CONTROL DE APROBACIÓN

Elaboró	Revisó	Aprobó
Ronaldo Enrrique Cárcamo Vásquez Alex Gerardo Gámez Arteaga	Jefe de Proyectos y Desarrollo	Gerente de Tecnología y Comunicaciones
__/__/__	__/__/__	__/__/__

8. CONTROL DE CAMBIOS

Versión	Cambios realizados	Aprobación Consejo de Administración	Número de Acta
1.0.0	Emisión inicial de la política. Establecimiento del marco normativo de gestión de incidencias de software basado en ITIL 4 y COBIT 2019.	__/__/__	Acta No. __

9. ANEXOS

Forman parte integral del presente documento los siguientes anexos:

- Anexo 1:** Acta de Aprobación de la Política Institucional de Gestión de Incidencias de Software.
- Anexo 2:** Flujo formal de siete etapas del proceso de gestión de incidencias de software.
- Anexo 3:** Matriz de criticidad, acuerdos de nivel de servicio y reglas de escalamiento.
- Anexo 4:** Matriz RACI de roles y responsabilidades por etapa del proceso.
- Anexo 5:** Fichas técnicas del tablero de indicadores clave de desempeño.

ANEXO 8: INSTRUMENTO DE ENCUESTA AUTOMÁTICA DE SATISFACCIÓN POSTERIOR AL CIERRE

Propósito del instrumento

El presente anexo desarrolla el instrumento institucional mediante el cual el modelo operacionaliza la medición de la satisfacción del colaborador reportante posterior al cierre formal de la incidencia, conforme a lo dispuesto en la Etapa 7 del flujo. El instrumento adopta la metodología del Customer Satisfaction Score, reconocida por ITIL 4 como práctica estándar de retroalimentación al usuario en la gestión de incidentes (IBM, 2023). Su finalidad es triple: alimentar de manera continua el indicador de satisfacción del tablero gerencial del componente, identificar oportunidades de mejora operativa derivadas de la experiencia real del usuario y constituir una vía formal de retroalimentación que complemente la certificación técnica realizada durante la Etapa 7.

Mecánica de envío automático

Tabla 80. Parámetros operativos del envío automático de la encuesta.

Parámetro	Definición operativa
Disparador automático	Cambio del ticket al estado "Cerrado" en ManageEngine ServiceDesk Plus
Destinatario	Colaborador reportante registrado como titular del ticket
Canal de envío	Correo electrónico institucional con enlace seguro al formulario embebido en la plataforma
Ventana de respuesta	Tres días hábiles posteriores a la recepción del envío inicial
Recordatorio automático	Un único recordatorio enviado al cumplirse el cincuenta por ciento de la ventana de respuesta, sin respuesta registrada
Anonimato relativo	Respuesta vinculada al ticket pero no al nombre del colaborador en los reportes consolidados, conforme al principio de retroalimentación honesta
Trazabilidad institucional	La encuesta queda asociada al expediente del ticket en la plataforma para fines de auditoría, sin exposición individual del reportante en los tableros

Fuente: Elaboración propia.

Cuestionario base. El cuestionario consta de cinco ítems, cuatro de ellos evaluables mediante escala Likert de cinco niveles y uno de texto libre opcional. La escala adoptada es la siguiente:

Tabla 81. Escala Likert aplicable a los ítems evaluables.

Valor	Descripción cualitativa
5	Totalmente satisfecho
4	Satisfecho
3	Neutral
2	Insatisfecho
1	Totalmente insatisfecho

Fuente: Elaboración propia.

Tabla 82. Cuestionario base de la encuesta de satisfacción.

#	Dimensión evaluada	Pregunta	Tipo de respuesta
P-01	Oportunidad de la atención	¿Qué tan satisfecho se encuentra con el tiempo total transcurrido entre el reporte de su incidencia y la resolución final?	Likert 1 a 5
P-02	Calidad de la comunicación	¿Qué tan satisfecho se encuentra con la claridad, oportunidad y suficiencia de la información recibida durante el proceso de atención?	Likert 1 a 5
P-03	Eficacia de la solución	¿Qué tan satisfecho se encuentra con la solución aplicada frente a la afectación operativa que originalmente reportó?	Likert 1 a 5
P-04	Satisfacción global	¿Qué tan satisfecho se encuentra, de manera global, con el servicio prestado por el área de Tecnología y	Likert 1 a 5

#	Dimensión evaluada	Pregunta	Tipo de respuesta
		Comunicaciones en la atención de esta incidencia?	
P-05	Retroalimentación cualitativa	¿Desea agregar algún comentario que permita mejorar el servicio? Indique observaciones específicas sobre el caso atendido.	Texto libre, opcional, hasta quinientos caracteres

Fuente: Elaboración propia.

Cálculo del indicador y umbral de alerta. El indicador de satisfacción del ticket se calcula como el promedio aritmético simple de los cuatro ítems Likert evaluables (P-01 a P-04), conforme a la siguiente fórmula:

$$\text{CSAT del ticket} = (P-01 + P-02 + P-03 + P-04) / 4$$

El indicador consolidado mensual se calcula como el promedio aritmético de los CSAT de todos los tickets cerrados durante el mes con encuesta respondida.

Tabla 83. Umbrales institucionales de interpretación del CSAT.

Rango del CSAT del ticket	Interpretación institucional	Acción automática asociada
Mayor o igual a 4.0	Satisfacción adecuada	Registro en el tablero del componente 6.5, sin acción adicional
Mayor o igual a 3.0 y menor a 4.0	Satisfacción aceptable con oportunidad de mejora	Registro en el tablero y consolidación para análisis de tendencia mensual
Menor a 3.0	Satisfacción insuficiente	Notificación automática al Jefe de Proyectos y Desarrollo para revisión obligatoria del caso dentro de cinco días hábiles, con análisis de causas y plan de acción documentado

Fuente: Elaboración propia.

Reglas institucionales de operación del instrumento. Tres reglas rigen la operación del instrumento durante el ciclo de vida del modelo.

Primero, **principio de no obligatoriedad de respuesta:** La encuesta es de respuesta voluntaria por parte del colaborador, dado que el carácter coercitivo comprometería la validez del dato obtenido; sin embargo, su envío automático es obligatorio para todo ticket cerrado, sin excepción.

Segundo, **principio de separación entre certificación y satisfacción:** La certificación formal de la solución, descrita en la Etapa 7, no se sustituye ni se condiciona por la respuesta a la encuesta; ambos instrumentos operan de manera independiente y miden dimensiones distintas del caso.

Tercero, **principio de revisión periódica del instrumento:** La pertinencia de las preguntas, los umbrales de alerta y la frecuencia de consolidación se revisan anualmente por el jefe de Proyectos y Desarrollo, con propuesta de ajuste a la Gerencia de Tecnología y Comunicaciones cuando la evidencia operativa lo justifique.