FACULTAD DE POSTGRADO
TRABAJO FINAL DE GRADUACIÓN

"DESARROLLO DE UN PLAN DE CONTINGENCIA Y RESPUESTA EFICAZ ANTE CIBERATAQUES DE TIPO RANSOMWARE EN EMPRESAS DE HONDURAS"

SUSTENTADO POR:

EDUARDO JOSE AVILA CALIX
RAMON HUMBERTO VENTURA RODRÍGUEZ

PREVIA INVESTIDURA AL TÍTULO DE

MÁSTER EN
GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN

TEGUCIGALPA, FRANCISCO MORAZÁN, HONDURAS, C.A.

MAYO, 2025

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

“DESARROLLO DE UN PLAN DE CONTINGENCIA Y RESPUESTA EFICAZ ANTE CIBERATAQUES DE TIPO RANSOMWARE EN EMPRESAS DE HONDURAS”

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TITULO DE MÁSTER EN

GESTIÓN EN TECNOLOGIAS DE LA INFORMACIÓN

ASESOR METODOLÓGICO

JESÚS RICARDO RODRÍGUEZ RIVERA

MEIMBROS DE LA TERNA:

JULISSA JAMILETH CORTES OSORTO

DAVID ANTONIO DIAZ GIRON

JOSUE DAVID MEJIA RIVERA

FACULTAD DE POSTGRADO

“DESARROLLO DE UN PLAN DE CONTINGENCIA Y RESPUESTA EFICAZ ANTE CIBERATAQUES DE TIPO RANSOMWARE EN EMPRESAS DE HONDURAS”

Eduardo Jose Avila Calix
Ramon Humberto Ventura Rodríguez

Resumen

En la actualidad, el ransomware se ha convertido en una de las principales amenazas de ciberseguridad para las empresas, afectando la continuidad operativa, la integridad de los datos y la estabilidad financiera. En Honduras, muchas organizaciones carecen de planes de contingencia y respuesta efectivos, lo que las hace vulnerables a ataques que pueden paralizar sus sistemas y exigir pagos de rescate para recuperar la información. Este estudio tuvo como objetivo desarrollar un plan de contingencia y respuesta eficaz ante este tipo de ciberataques. Para ello, se identificaron las principales vulnerabilidades y factores de riesgo a través de un análisis cualitativo y descriptivo, la investigación permitió evidenciar que la falta de inversión en seguridad informática, la ausencia de protocolos claros y el desconocimiento de las mejores prácticas incrementan el riesgo de sufrir estos ataques. Como resultado, se diseñó un **Plan de Contingencia y Respuesta**, basado en **estrategias de prevención, detección, respuesta y recuperación** ante incidentes de ransomware. La aplicación de este plan permitirá a las empresas **fortalecer su resiliencia cibernética**, minimizar el impacto de los ataques y garantizar la continuidad operativa.

Palabras claves: (Ransomware, ciberseguridad, contingencia, continuidad, gestión, incidentes, prevención, ciberataques)

GRADUATE SCHOOL

“DEVELOPMENT OF A CONTINGENCY PLAN AND EFFECTIVE RESPONSE TO RANSOMWARE-TYPE CYBERATTACKS IN HONDURAN COMPANIES”

Eduardo Jose Avila Calix
Ramon Humberto Ventura Rodríguez

Abstract

Currently, ransomware has become one of the main cybersecurity threats for companies, affecting operational continuity, data integrity, and financial stability. In Honduras, many organizations lack effective contingency and response plans, making them vulnerable to attacks that can cripple their systems and demand ransom payments to recover information. This study aimed to develop an effective contingency and response plan against this type of cyberattack. To achieve this, the main vulnerabilities and risk factors were identified through a qualitative and descriptive analysis. The research revealed that the lack of investment in cybersecurity, the absence of clear protocols, and the lack of awareness of best practices increase the risk of these attacks. As a result, a **Contingency and Response Plan** was designed, based on prevention, detection, response, and recovery strategies against ransomware incidents. The implementation of this plan will enable companies to strengthen their cybersecurity resilience, minimize the impact of attacks, and ensure operational continuity.

Keywords: (Ransomware, cybersecurity, contingency, continuity, management, incidents, prevention, cyberattacks)

DEDICATORIA

Dedico este trabajo de tesis a mis hermanos Andrea, Jimena y Flavio, en especial a mi madre Flavia Calix, por todo su amor, sacrificio y constante apoyo en cada paso de mi formación académica. A mi tío Adolfo Calix (Q.E.P.D), también a mis amigos y colegas, quienes me han acompañado en este camino, brindándome palabras de aliento en los momentos de mayor desafío.

Eduardo Calix.

Dedico este trabajo con profundo amor y gratitud a mi madre Carolina Rodríguez, cuyo esfuerzo y sacrificio han sido mi mayor inspiración, y a mis hermanos Ángel Rodríguez e Israel Ventura, quienes con su apoyo incondicional y compañía han sido una fuente constante de fortaleza y motivación. Sin ustedes, este logro no habría sido posible.

Ramón Ventura.

AGRADECIMIENTO

Agradezco profundamente a Dios, por brindarme la fortaleza y la perseverancia para culminar este trabajo de investigación. A mi familia, por su apoyo incondicional, paciencia y motivación en cada etapa de este proceso. A mi novia Arling Flores por escucharme y apoyarme para que pueda alcanzar este logro. A mis tíos Angelica y Gonzalo Calix, por ser siempre motores de apoyo en mi vida. A mi amiga Loreste Portillo por sus consejos y cariño. Al profesor Carlos Lanza por todo lo brindado en mis procesos de aprendizaje. A mis profesores y asesor Ricardo Rodríguez de la Maestría en Gestión de Tecnologías de la Información, por compartir sus conocimientos y guiarme en el desarrollo de este trabajo. También, expreso mi gratitud a Ramón Ventura por su compañerismo, dedicación y empeño en este trabajo.

Eduardo Calix.

Agradezco, en primer lugar, a Dios, por darme la fuerza y la perseverancia para alcanzar esta meta. A mi madre, por su amor incondicional, sacrificio y guía en cada paso de mi vida. A mis hermanos, por su apoyo y compañía, que han sido un pilar fundamental en este camino. También extiendo mi gratitud a quienes, de una u otra manera, contribuyeron con su conocimiento, consejos y palabras de aliento para la realización de este trabajo.

Ramon Ventura.

ÍNDICE DE CONTENIDO

DEDICATORIA ix
AGRADECIMIENTO xi
ÍNDICE DE CONTENIDO xiii
ÍNDICE DE TABLAS xvi
ÍNDICE DE FIGURAS xvi
CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN 1
1.1 INTRODUCCIÓN 1
1.2 ANTECEDENTES DEL PROBLEMA 2
1.3 PLANTEAMIENTO DEL PROBLEMA 5
1.4 PREGUNTAS DE INVESTIGACIÓN 6
1.4.1 PREGUNTA GENERAL 6
1.4.2 PREGUNTAS ESPECÍFICAS 6
1.5 OBJETIVOS 6
1.5.1 OBJETIVO GENERAL 6
1.5.2 OBJETIVOS ESPECÍFICOS 6
1.6 JUSTIFICACIÓN 6
CAPÍTULO II – MARCO TEÓRICO 8
2.1 MACROENTORNO 9
2.1.1 ENTORNO ECONÓMICO 12
2.1.2 ENTORNO TECNOLÓGICO 12
2.1.3 ENTORNO SOCIAL 13
2.1.4 ENTORNO LEGAL 15
2.2 MICROENTORNO 16
2.2.1 PERSPECTIVA CENTROAMERICANA 16
2.2.2 PERSPECTIVA HONDUREÑA 17
2.3 TEORÍAS DE SUSTENTO 20
2.3.1 MODELO DE CIBERSEGURIDAD EN PROFUNDIDAD 20
2.3.2 INTELIGENCIA DE AMENAZAS Y RESPUESTA PROACTIVA 21
2.4 METODOLOGÍAS TEMÁTICAS 22

2.4.1 ANÁLISIS DE RIESGOS 22
2.4.2 METODOLOGÍA PARA EL DESARROLLO DE PLANES DE CONTINGENCIA 22
2.5 HERRAMIENTAS 24
2.5.1 HERRAMIENTAS OFIMÁTICAS 24
2.5.2 HERRAMIENTAS DE PLANIFICACIÓN 25
2.5.3 HERRAMIENTAS DE MENSAJERÍA INSTANTÁNEA 26
2.5.4 HERRAMIENTAS DE REUNIONES Y VIDEO LLAMADAS 27
2.5.5 HERRAMIENTAS DE ANÁLISIS Y VISUALIZACIÓN DE DATOS 27
2.6 CONCEPTUALIZACIÓN 28
2.7 MARCO LEGAL 31
2.7.1 MARCO LEGAL INTERNACIONAL 31
2.7.2 MARCO LEGAL NACIONAL 33
CAPÍTULO III – METODOLOGÍA DE LA INVESTIGACIÓN 35
3.1 ENFOQUE 35
3.2 ALCANCE 37
3.3 DISEÑO 38
3.3.1 POBLACIÓN 39
3.3.2 MUESTRA 39
3.3.3 TÉCNICAS DE MUESTREO 40
3.4 CRITERIOS DE SELECCIÓN DE LA MUESTRA 40
3.4.1 CRITERIOS DE INCLUSIÓN 40
3.4.2 CRITERIOS DE EXCLUSIÓN 41
3.5 HIPÓTESIS (No aplica) 42
3.6 OPERACIONALIZACIÓN DE LAS VARIABLES 43
3.7 TÉCNICAS, INSTRUMENTOS Y PROCEDIMIENTOS APLICADOS 43
3.7.1 TÉCNICAS 43
3.7.2 INSTRUMENTOS 44
3.7.3 PROCEDIMIENTOS 44
3.7.4 PLAN DE ANÁLISIS 45
3.8 FUENTES DE INFORMACIÓN 46
3.8.1 FUENTES PRIMARIAS 46

3.8.2 FUENTES SECUNDARIAS 47
3.9 MATRIZ DE CONGRUENCIA 48
CAPÍTULO IV – RESULTADOS Y ANALISIS 49
4.1 ANÁLISIS EXPLORATORIO DE DATOS 49
4.1.1 DESCRIPCIÓN GENERAL DEL CONJUNTO DE DATOS 49
4.1.2 LIMPIEZA Y PREPARACIÓN DE DATOS 50
4.1.3 VISUALIZACIÓN DE DATOS 53
4.2 INFORME DE PROCESO DE RECOLECCIÓN DE DATOS 77
4.2.1 DESCRIPCIÓN DEL PROCESO 77
4.2.2 PARTICIPANTES 78
4.2.3 INSTRUMENTOS UTILIZADOS 78
4.2.4 CONSIDERACIONES ÉTICAS 79
4.3 ANÁLISIS INFERENCIAL Y MODELOS APLICADOS 79
4.3.1 TIPOS DE MODELOS APLICADOS 79
4.3.2 VISUALIZACIÓN DE MODELOS 80
CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES 87
5.1 CONCLUSIONES 87
5.2 RECOMENDACIONES 88
CAPÍTULO VI. APLICABILIDAD 90
6.1 NOMBRE DE LA PROPUESTA 90
6.2 JUSTIFICACIÓN DE LA PROPUESTA 90
6.3 ALCANCE DE LA PROPUESTA 91
6.4 DESCRIPCIÓN Y DESARROLLO 92
6.4.1 DESCRIPCIÓN 92
6.4.2 DESARROLLO 93
6.5 MEDIDAS DE CONTROL 105
6.5.1 INDICADORES 106
6.5.2 PLAN DE SEGUIMIENTO 108
6.6 CRONOGRAMA DE IMPLEMENTACIÓN Y PRESUPUESTO 108
6.6.1 CRONOGRAMA DE IMPLEMENTACIÓN 109
6.6.2 PRESUPUESTO 110

6.7 CONCORDANCIA 112
REFERENCIAS BIBLIOGRÁFICAS 116
ANEXOS 119

ÍNDICE DE TABLAS

Tabla 1 Herramientas Ofimáticas ____ 24
Tabla 2 Herramientas de Planificación ____ 25
Tabla 3 Herramientas de Mensajería Instantánea ____ 26
Tabla 4 Herramientas de Reuniones y Video llamadas ____ 27
Tabla 5 Herramientas de Análisis de Datos ____ 27
Tabla 6 Legislación Internacional ____ 32
Tabla 7 Legislación de Honduras ____ 33
Tabla 8 Operacionalización de las variables ____ 43
Tabla 9 Plan de análisis de la investigación ____ 45
Tabla 10 Matriz de congruencia ____ 48
Tabla 11 Variables Bajo Estudio ____ 50
Tabla 12 Comparativa de Modelos Supervisados ____ 84
Tabla 13 Lista de comprobación para la protección proactiva ____ 97
Tabla 14 Replicabilidad en otros contextos ____ 105
Tabla 15 Indicadores claves de desempeño ____ 106
Tabla 16 Seguimiento de Medidas de Control ____ 108
Tabla 17 Cronograma de implementación ____ 109
Tabla 18 Presupuesto estimado para el plan ____ 111
Tabla 19 Recomendaciones para Pequeñas y Medianas Empresas ____ 112
Tabla 20 Concordancia de los capítulos ____ 114

ÍNDICE DE FIGURAS

Figura 1 Elementos de un Programa de Ciberseguridad. 10

Figura 2 Porcentaje y comparación de Organizaciones afectadas por el malware semanalmente en Latam y Honduras. 11
Figura 3 Porcentaje de Organizaciones afectadas por el ransomware en el último año. 12
Figura 4 Elementos de un Programa de Ciberseguridad. 13
Figura 5 Elementos de un Programa de Ciberseguridad. 14
Figura 6 La ciberseguridad genera valor en toda la empresa 15
Figura 7 El Círculo de Deming (Shewhart): Ciclo PDCA (PHVA) 24
Figura 8 Importación de Pandas 51
Figura 9 Columnas con Nombres Originales 51
Figura 10 Columnas con Nombres Modificados 52
Figura 11 Valores Faltantes por Columna 52
Figura 12 Mapa de Valores Faltantes 53
Figura 13 Cantidad de Empresas por Sector 54
Figura 14 Cantidad de Empleados por Numero 55
Figura 15 Disponibilidad de Equipo de Ciberseguridad 56
Figura 16 Victimas por Ransomware 57
Figura 17 Como se manejó la situación. 58
Figura 18 Medidas Preventivas Utilizadas 59
Figura 19 Actualización de Políticas de Ciberseguridad 60
Figura 20 Acciones Como Prioridad 1 Ante Ransomware 62
Figura 21 Acciones Como Prioridad 2 Ante Ransomware 62
Figura 22 Acciones Como Prioridad 3 Ante Ransomware 63
Figura 23 Acciones Como Prioridad 4 Ante Ransomware 63
Figura 24 Acciones Como Prioridad 5 Ante Ransomware 64
Figura 25 Uso de Sistemas de Respaldo 65
Figura 26 Disponibilidad de un Plan de Contingencia 66
Figura 27 Barreras que Impiden Mejorar la Ciberseguridad 67
Figura 28 Nivel de Conciencia en Honduras 68
Figura 29 Estrategias para Fortalecer la Ciberseguridad 69
Figura 30 Histograma Empresas 70
Figura 31 Histograma Número de Empleados 71

Figura 32 Histograma Equipo de Ciberseguridad 71
Figura 33 Histograma de Victimas de Ransomware 72
Figura 34 Histograma de Políticas 73
Figura 35 Histograma de Respaldos 73
Figura 36 Histograma de Plan de Contingencia 74
Figura 37 Ataques de Ransomware por Empresa 75
Figura 38 Ataques de Ransomware por Cantidad de Empleados 75
Figura 39 Ataques de Ransomware por Frecuencia de Respaldos 76
Figura 40 Matriz de Correlación 77
Figura 41 Árbol de decisión 80
Figura 42 Matriz de Confusión de Árbol de Decisión 81
Figura 43 Matriz de Confusión de Regresión Logística 82
Figura 44 Matriz de Confusión de Gradient Boosting 83
Figura 45 Grafico de Curva ROC 84
Figura 46 Método del Codo para Obtener Numero de Clusteres 85
Figura 47 Clustering por K-Means 85
Figura 48 Ciclo PHVA enfocado en la ISO 27001 92
Figura 49 Ransomware 93
Figura 50 Diagrama de Flujo de Prevención 100
Figura 51 Diagrama de Flujo de Detección 101
Figura 52 Diagrama de Flujo de Respuesta 103
Figura 53 Diagrama de Flujo de Recuperación 105

ÍNDICE DE ANEXOS

Anexo 1 Encuesta realizada para recopilar información _____ 119
Anexo 2 Entrevista realizada a especialista de ciberseguridad de Checkpoint _____ 122
Anexo 3 Encuesta finalizada _____ 124
Anexo 4 Importación de Archivo CSV _____ 124
Anexo 5 Análisis de Valores Faltantes _____ 124
Anexo 6 Árbol de Decisión _____ 124

Anexo 7 Regresión Logística _____ 125
Anexo 8 Gradient Boosting _____ 125
Anexo 9 Clustering por K-Means _____ 125
Anexo 10 Comparación de Modelos con Curva ROC _____ 126

CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 INTRODUCCIÓN

En la presente era digital se han venido presentando cambios significativos en el hecho de como usamos el internet y la información en línea, los ataques de tipo ransomware se han convertido en una de las amenazas más devastadoras para las empresas a nivel mundial. Estos ataques, que comprometen la integridad de los datos y llegan a paralizar las operaciones, han generado pérdidas significativas tanto en términos económicos como de reputación empresarial. En el contexto de Honduras, muchas empresas han comenzado a adoptar tecnologías avanzadas, lo que incrementa la exposición a ciberataques, pero, en su mayoría, carecen de planes de contingencia y respuesta adecuados para mitigar los riesgos asociados al ransomware en específico.

El estado actual de la ciberseguridad en el país presenta serios desafíos. A medida que las empresas locales avanzan en la adopción de tecnologías y procesos digitales, aumentan también su vulnerabilidad ante ciberataques, sin embargo, la mayoría de las empresas en el país carecen de estrategias robustas para hacer frente a incidentes de ransomware. Informes de ciberseguridad en la región centroamericana, junto con casos reportados por medios nacionales, sugieren que muchas empresas hondureñas enfrentan limitaciones significativas en términos de recursos y conocimiento especializado, lo cual dificulta la implementación de planes de contingencia y respuesta eficaces.

Este trabajo se propone desarrollar un plan de contingencia y respuesta que permita a las empresas en Honduras enfrentar estos desafíos de manera efectiva. La investigación analizará el estado actual de la seguridad cibernética en el entorno empresarial hondureño, identificará las mejores prácticas a nivel global y adaptará soluciones específicas que se ajusten a las necesidades y limitaciones del contexto local. Al generar un modelo de respuesta ante ransomware adaptado a la realidad nacional, esta investigación busca fortalecer la capacidad de las empresas hondureñas para mitigar el impacto de estos ciberataques y asegurar la continuidad operativa.

En el marco teórico, se aborda la ciberseguridad desde diferentes perspectivas, incluyendo el análisis de normativas internacionales como ISO 22301 e ISO 27001, que establecen lineamientos para la gestión de continuidad del negocio y la seguridad de la información. También se exploran conceptos clave como las estrategias de defensa en profundidad y la inteligencia de

amenazas, los cuales fundamentan las medidas propuestas en el plan de contingencia.

La metodología de investigación adoptada es cualitativa con un alcance descriptivo. Este enfoque permite recopilar y analizar información detallada sobre las prácticas actuales de ciberseguridad, los factores de riesgo y las vulnerabilidades en las empresas hondureñas. Se utilizarán entrevistas a profundidad y análisis de documentos como técnicas principales, con el objetivo de identificar patrones y tendencias en la preparación de las organizaciones ante ataques de ransomware. Este enfoque no solo ayudará a caracterizar el problema, sino también a diseñar soluciones prácticas y ajustadas a la realidad nacional.

Para consolidar los hallazgos de esta investigación, el capítulo de Resultados y Análisis recopila y presenta la información obtenida a través de entrevistas con expertos en ciberseguridad, estudios de casos y revisión documental. A partir de estos datos, se identifican las vulnerabilidades más críticas que enfrentan las empresas hondureñas ante ataques de ransomware, así como las estrategias actualmente implementadas para mitigar sus efectos. Además, se analizan patrones comunes en la respuesta de las organizaciones frente a estos incidentes, evaluando la efectividad de sus planes de contingencia. Este análisis proporciona una base fundamentada para el diseño de un modelo de respuesta más eficiente, alineado con las necesidades del contexto hondureño y sustentado en las mejores prácticas internacionales de ciberseguridad.

En este sentido, la aplicabilidad de la investigación se concreta en el desarrollo de un plan de contingencia y respuesta ante ransomware, diseñado específicamente para el entorno empresarial hondureño. Este plan propone medidas de prevención, detección, respuesta y recuperación, integrando herramientas de gestión y estrategias organizacionales adaptadas a distintos tipos de empresas. Su implementación busca fortalecer la resiliencia corporativa frente a amenazas cibernéticas, proporcionando lineamientos claros y efectivos que puedan ser replicados y ajustados a diversas realidades empresariales.

Con esta estructura, la investigación no solo busca contribuir al fortalecimiento de la ciberseguridad en Honduras, sino también sentar un precedente para futuros estudios e iniciativas que promuevan un entorno digital más seguro y resiliente.

1.2 ANTECEDENTES DEL PROBLEMA

Según el artículo de Nagar (2024), los primeros registros de ransomware datan de 1989

con la aparición del Troyano AIDS, desarrollado por el Dr. Joseph Popp, un biólogo graduado de Harvard. Este malware fue distribuido a través de 20,000 disquetes enviados a los asistentes de una conferencia sobre el SIDA organizada por la Organización Mundial de la Salud. Una vez insertado en una computadora, el virus permanecía inactivo hasta después de 90 reinicios, momento en el que cifraba los archivos del disco duro y exigía un pago de 189 dólares para su descifrado.

A mediados de los años 2000, Nagar (2024) menciona que, a medida que evolucionaron los ataques de ransomware, comenzaron a utilizar técnicas de cifrado más avanzadas y estrategias sofisticadas para evadir la detección por parte de los dispositivos y usuarios. Este periodo representó un punto de inflexión, pasando de métodos rudimentarios a tácticas altamente especializadas por parte de los atacantes. Ejemplos notables de esta evolución fueron Gpcode (2004) y Archivius (2006), los cuales implementaron el cifrado RSA en lugar de AES, mejorando significativamente la seguridad del bloqueo de archivos. Además, fue en esta etapa cuando los delincuentes comenzaron a exigir pagos en bitcoin para la liberación de la información, una práctica que posteriormente se convirtió en un estándar en ataques de ransomware modernos.

A finales de los años 2000 y a principios del 2010, Nagar (2024) en su libro enfatiza que, con el avance de las técnicas de ransomware, estos dejaron de ser programas maliciosos fáciles de eliminar y comenzaron a utilizar cifrados más robustos, haciéndolos prácticamente irrecuperables sin la clave de descifrado. Además, los atacantes mejoraron sus mecanismos para evadir la detección de los antivirus, utilizando estrategias como la ofuscación de código y la ejecución en memoria para evitar ser identificados por los sistemas de seguridad. En esta época sobresalen los ransomware: CryptoLocker (2013) y CryptoWall (2014), ambos empleaban los algoritmos RSA-2048 y AES-256 para cifrar la información y su distribución era mediante los correos de phishing los cuales contenían archivos adjuntos con el código malicioso, lo cual afecto a millones de dispositivos.

A mediados del año 2010, Nagar (2024) afirma que, el ransomware ya contaba con una estructura bien definida, basada en un malware capaz de cifrar información y exigir un pago para su liberación. Sin embargo, a partir de 2015 surgió un cambio significativo en la forma en que se distribuía este tipo de amenaza. Con la aparición de Tox (2015) y Cerber (2016), se implementó un nuevo modelo de negocio denominado "Ransomware como Servicio" (RaaS, por sus siglas en

inglés), el cual permitía a ciberdelincuentes sin conocimientos avanzados en programación adquirir y distribuir ransomware a cambio de una comisión sobre los pagos obtenidos. Este modelo facilitó la proliferación de ataques, ya que eliminó la necesidad de que los atacantes desarrollaran su propio malware, permitiéndoles enfocarse únicamente en su distribución y ejecución.

A inicios de la década del 2020, según Nagar (2024), la doble extorsión implicaba no solo cifrar los archivos de la víctima, sino también amenazar con divulgar la información robada en Internet si no se realizaba el pago del rescate. Esta táctica aumentó la presión sobre las víctimas, llevándolas a ceder ante las exigencias de los atacantes. Por otro lado, los ataques dirigidos marcaron un cambio en la estrategia de los ciberdelincuentes, quienes comenzaron a planificar y ejecutar ataques específicamente contra organizaciones gubernamentales, hospitales, infraestructuras críticas y empresas estratégicas. Estas entidades se convirtieron en objetivos clave debido al valor de sus datos y la urgencia de restaurar sus sistemas. Este tipo de ataque evidenció la creciente profesionalización del ransomware, consolidándolo como una de las amenazas cibernéticas más peligrosas a nivel global.

Durante la pandemia del COVID 19 en el año 2020, muchas empresas a nivel global no estaban preparadas para implementar trabajo remoto, lo cual provocó que estas mismas utilizaran protocolos inseguros o mal configurados para brindar acceso remoto a sus colaboradores. Solo en Latinoamérica, en el mes de abril se registraron 90 millones de ataques de “escritorio remoto” siendo este el mes con mayor registro de ataques durante este año. Sin embargo, a finales del 2020, los ataques de ransomware disminuyeron llegando a menos del millón, esto debido a que las victimas ya no eran elegidas al azar, sino seleccionadas cuidadosamente por los atacantes, las cuales en su mayoría eran grandes empresas que a lo mejor estuvieran dispuestas a pagar el rescate de la información (*América Latina en 2020*, 2020).

En Honduras, según la CONATEL (2020), se emitió una alerta sobre la propagación de CovidLock, un ransomware diseñado para atacar dispositivos móviles. Este malware se presentaba como una aplicación de salud que prometía ayudar a prevenir el contagio de COVID-19, notificando a los usuarios sobre casos cercanos mediante un mapa de calor. Sin embargo, una vez instalado en el dispositivo, CovidLock bloqueaba la pantalla y exigía un pago de 100 dólares en bitcoin a cambio de la contraseña de desbloqueo. Este incidente evidenció cómo los ciberdelincuentes aprovecharon la incertidumbre generada por la pandemia para distribuir

ransomware a través de aplicaciones fraudulentas. Además, resaltó la necesidad de fortalecer la ciberseguridad en dispositivos móviles y concienciar a los usuarios sobre los riesgos de descargar aplicaciones de fuentes no verificadas.

El 02 de febrero del 2024, la empresa de telecomunicaciones Claro informó a través de sus redes sociales que había sido víctima de un ataque de ransomware que afectó sus operaciones en varios países de Centroamérica, incluyendo Honduras. La compañía detectó actividad anómala en sus sistemas el 25 de enero, lo que llevó a la suspensión temporal de servicios como plataformas de consulta, recarga de saldo y pago de servicios, mientras se trabajaba en la solución del incidente (revistaeyn.com, 2024).

1.3 PLANTEAMIENTO DEL PROBLEMA

El incremento en la frecuencia y sofisticación de los ciberataques, específicamente de tipo ransomware, pone de manifiesto la necesidad urgente de estrategias efectivas de respuesta y recuperación en las empresas de Honduras. A pesar del creciente riesgo, la mayoría de las empresas hondureñas carecen de planes de contingencia y protocolos de respuesta sólidos, lo que las expone a severas consecuencias en términos de pérdida de datos, paralización de operaciones, y daños irreparables a su reputación en el mercado.

En Honduras, las debilidades más comunes que aumentan la susceptibilidad a ataques de ransomware incluyen infraestructura tecnológica limitada, estamos en el lugar 129 de índice de desarrollo de las TIC y en el lugar 178 del Índice mundial de ciberseguridad, según NCSI (2022), la falta de personal especializado en ciberseguridad y los presupuestos reducidos destinados a protección informática son factores que incrementan la vulnerabilidad de las empresas ante ciberataques. Además, la escasez de información local sobre incidentes previos dificulta la adopción de medidas preventivas efectivas. Muchas organizaciones continúan operando con software y hardware obsoletos, lo que facilita el acceso no autorizado y pone en riesgo la seguridad de datos críticos. Esta combinación de factores deja a las empresas expuestas a ataques como el ransomware, que aprovecha brechas de seguridad y fallos en la infraestructura tecnológica.

El principal problema abordado en esta investigación es la falta de un plan de contingencia y respuesta eficaz ante ataques de ransomware en empresas hondureñas, lo que compromete la continuidad operativa, la integridad de los datos y la confianza de clientes y socios. Esta investigación busca desarrollar un modelo que no solo contemple una respuesta reactiva, sino

también estrategias de prevención y recuperación proactiva. Su implementación proporcionará a las empresas una herramienta práctica para gestionar incidentes de ransomware de manera efectiva, reduciendo el impacto operativo y financiero de estos ataques (Check Point Research, 2022).

1.4 PREGUNTAS DE INVESTIGACIÓN

1.4.1 PREGUNTA GENERAL

¿Cómo pueden las empresas en Honduras desarrollar e implementar un plan de contingencia y respuesta eficaz para mitigar el impacto de ciberataques de tipo ransomware y garantizar la continuidad de sus operaciones?

1.4.2 PREGUNTAS ESPECÍFICAS

¿Cuáles son las principales vulnerabilidades y factores de riesgo que enfrentan las empresas hondureñas ante ataques de ransomware?

¿Qué componentes deben incluirse en un plan de contingencia eficaz para minimizar los daños causados por ciberataques de tipo ransomware?

1.5 OBJETIVOS

1.5.1 OBJETIVO GENERAL

Desarrollar un plan de contingencia y respuesta eficaz ante ciberataques de tipo ransomware para las empresas en Honduras, con el fin de reducir el impacto de estos incidentes y garantizar la continuidad operativa y la integridad de la información.

1.5.2 OBJETIVOS ESPECÍFICOS

- Identificar las principales vulnerabilidades y factores de riesgo en las empresas hondureñas frente a los ataques de tipo ransomware.
- Diseñar un plan de contingencia que contemple medidas preventivas, de detección, respuesta y recuperación ante ataques de tipo ransomware.

1.6 JUSTIFICACIÓN

Los ataques de ransomware han generado graves incidentes de ciberseguridad a nivel mundial, causando importantes pérdidas económicas en diversas empresas. De acuerdo con

Kaspersky en su artículo, *América Latina en 2020* (2020), estos tipos de malware han evolucionado para enfocarse principalmente en organizaciones específicas, en lugar de usuarios individuales. Ante esto, resulta esencial la adopción de un marco estratégico que permita a las empresas fortalecer sus defensas y estar mejor preparadas para enfrentar este tipo de amenazas.

La relevancia y pertinencia de esta investigación radican en la creciente amenaza que los ciberataques de tipo ransomware representan para las empresas hondureñas. Debido a la rápida adopción de tecnologías digitales y a la falta de preparación en ciberseguridad, estas organizaciones se vuelven altamente vulnerables. La investigación aborda así un problema urgente en el contexto nacional y responde a una necesidad crítica: la creación de planes de contingencia efectivos que protejan la integridad de los datos y garanticen la continuidad operativa.

Además, esta investigación representa una contribución innovadora al área de ciberseguridad en Honduras, al adaptar las mejores prácticas internacionales a un contexto local específico. A diferencia de los modelos internacionales, que suelen estar diseñados para contextos con mayor acceso a recursos, este plan integrará soluciones prácticas y adaptadas a las capacidades y limitaciones del entorno empresarial hondureño. Incluirá medidas de recuperación rápida y protocolos de continuidad operativa, así como un componente de capacitación continua para la concienciación del personal en prácticas seguras. Estos elementos permitirán que las empresas cuenten con un modelo de ciberseguridad accesible y efectivo que no solo mitigue el impacto de los ataques, sino que también mejore la prevención y respuesta a largo plazo.

Un análisis reciente de Checkpoint (2024), revela patrones preocupantes en la ciberseguridad hondureña. Si bien la incidencia de ataques de ransomware en Honduras (1.1%) se encuentra por debajo del promedio latinoamericano (5.4%), existen amenazas mucho más frecuentes que deben ser atendidas. El país supera ampliamente el promedio regional en ataques a dispositivos móviles (2.2% frente a 1.0%), malware bancario (10.6% frente a 4.9%) y botnets (13.9% frente a 12.7%). Este panorama resalta la urgente necesidad de fortalecer la postura de ciberseguridad en empresas hondureñas, especialmente en sectores estratégicos como el financiero y de servicios móviles. Este enfoque es orientado a las necesidades locales, permitirá que las organizaciones hondureñas desarrollen la resiliencia necesaria ante el ransomware, aportando así un modelo innovador en ciberseguridad específicamente diseñado para el contexto de Honduras.

CAPÍTULO II – MARCO TEÓRICO

Se sustentará el desarrollo de un plan de contingencia y respuesta eficaz ante ciberataques de tipo ransomware para empresas en Honduras con la investigación realizada. En la primera sección se aborda el concepto de ransomware y sus implicaciones en el sector empresarial, mientras que en la segunda se describe el macroentorno, analizando factores sociales, económicos, tecnológicos y legales que inciden en el desarrollo de ciberseguridad a nivel latinoamericano y como repercuten en el país expuestas en el microentorno. Este marco de referencia permite comprender el contexto en el cual las empresas hondureñas operan y las vulnerabilidades a las que están expuestas, aportando una base sólida para diseñar estrategias de prevención y mitigación efectivas, con la cual hacer frente a los ataques tipo ransomware.

Según Samaniego-Mena et al, (2021), la ciberseguridad se ha convertido en uno de los mayores desafíos para las empresas en los últimos años. En 2019, más de 4,100 millones de registros fueron expuestos debido a filtraciones de datos, y el costo promedio de una violación de seguridad a nivel global ascendió a USD 3.92 millones. Con estas tendencias en aumento, se proyecta que el gasto mundial en ciberseguridad alcanzará los USD 110,990 millones para 2025, reflejando la creciente necesidad de fortalecer la protección digital en las organizaciones.

La pandemia de COVID-19 impulsó un aumento considerable en las amenazas de ciberseguridad, dejando a las empresas más expuestas a posibles ataques. En particular, el sector de tecnología financiera (FinTech) ha sido uno de los más afectados, registrando un incremento en los ciberataques desde el inicio de la crisis sanitaria. Además, los incidentes de phishing, ransomware y ataques relacionados con el coronavirus han experimentado un crecimiento significativo, evidenciando la urgencia de fortalecer las estrategias de protección digital en las organizaciones (Samaniego-Mena et al, 2021).

Además, la proliferación de las TIC ha afectado al ecosistema internacional más amplio dando vida a nuevas posibilidades organizativas, como los servicios de gobierno electrónico, y nuevas posibilidades económicas y productivas. Todos los países se ven afectados en cierta medida por la brecha digital y, como factor clave de la economía, la sociedad y el gobierno, que dependen de sistemas digitales, la ciberseguridad debería ser una alta prioridad (*Global Cybersecurity Index*, 2020).

Para Chauhan, et al (2015), un ransomware se define como: “un malware bastante

interesante que, después de infectar el sistema, bloquea algunos recursos populares e importantes del sistema informático y luego exige dinero de rescate para devolver el acceso" (p.206).

Samaniego-Mena, et al (2021), menciona lo siguiente: "el ransomware se ha convertido en una de las principales amenazas para las empresas debido a su capacidad para paralizar operaciones, robar información y generar significativas pérdidas económicas" (p.50).

Con la masificación de las tecnologías y el acceso a la red por parte de los usuarios, este ataque encuentra nuevas oportunidades para causar daño a las organizaciones y usuarios, ya que a la par de los avances tecnológicos y avances en cuanto a seguridad, el Ransomware también se adapta al entorno. Esto dio pie a la aparición de tres categorías: ransomware que cifra archivos, ransomware de pantalla de bloqueo y ransomware para dispositivos móviles.

2.1 MACROENTORNO

Se explica en el artículo de Ávila Niño (2023) que, en los últimos años América Latina ha sido blanco de cibercriminales que ejecutan campañas de ransomware, afectando tanto a organizaciones como a individuos. El aumento en los reportes de incidentes ante las autoridades de cada país evidencia un impacto creciente de este tipo de ataque. Ante esta problemática, se plantea la implementación de un compilado de buenas prácticas orientadas a fortalecer la seguridad digital y reducir la exposición de empresas y personas a esta modalidad de ciberdelito.

Ávila Niño (2023) también explica que, al ejecutarse un ransomware, el software malicioso toma control del sistema y bloquea el acceso a la información o los datos de la víctima, exigiendo un pago a cambio de su liberación. Este rescate, por lo general, se solicita en criptomonedas debido a su dificultad de rastreo. Aunque la extorsión basada en datos se remonta aproximadamente al año 2005, la evolución del software de cifrado y el auge de las criptomonedas han sido factores determinantes en el crecimiento y sofisticación de estos ataques.

Y no solo América Latina, para SOPHOS (2024), los ataques de ransomware han afectado a múltiples regiones del mundo, con un impacto significativo en Europa. Francia registró la tasa más alta de ataques en 2024, con un 74 % de las empresas encuestadas reportando incidentes en el último año, seguida de Sudáfrica (69 %) e Italia (68 %). En contraste, los países con menores índices de ataques fueron Brasil (44 %), Japón (51 %) y Australia (54 %), a nivel global, nueve países reportaron una reducción en los ataques en comparación con 2023, mientras que cinco

países europeos -Alemania, Austria, Francia, Italia y el Reino Unido- experimentaron un aumento. Este incremento podría atribuirse a un crecimiento en los ataques dirigidos contra organizaciones europeas o a la incapacidad de sus sistemas de defensa para mantenerse al ritmo de las estrategias avanzadas de los atacantes, versus otras regiones.

SOPHOS (2024), identifica que las organizaciones con mayores ingresos son las más propensas a sufrir ataques de ransomware, especialmente aquellas que superan los USD 5,000 millones en facturación, donde el 38 % de los incidentes se originan a partir de la vulneración de credenciales. A medida que una empresa expande su infraestructura tecnológica, esta se vuelve más extensa y difícil de proteger, incrementando los riesgos de seguridad. En compañías con ingresos entre USD 250-500 millones y USD 500-1,000 millones, el acceso no autorizado a credenciales es el método de ataque más común. Por otro lado, en organizaciones con ganancias menores el principal factor de riesgo viene de correos fraudulentos, los cuales representan el 49 % de los ataques en esta categoría. En términos generales, las estrategias basadas en phishing y correos maliciosos siguen siendo una de las técnicas más utilizadas por los ciberdelincuentes.

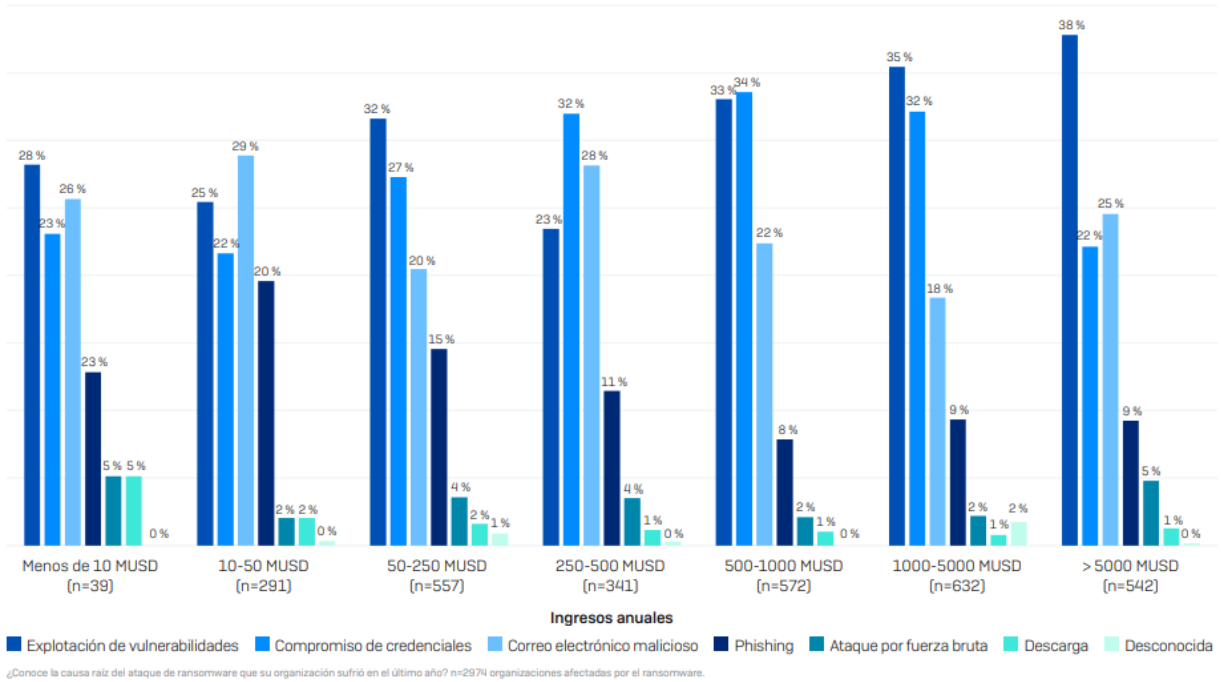


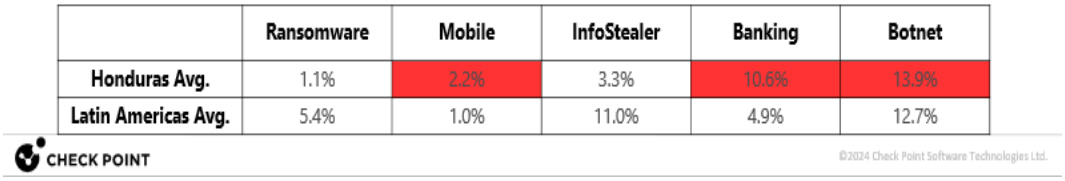
Figura 1 Elementos de un Programa de Ciberseguridad.
Fuente: SOPHOS (2024).

Según AO Kaspersky Lab (2024), las clases de ransomware más frecuentes son dos:

a) **Ransomware de bloqueo**. Este tipo de ransomware está diseñado para bloquear funciones básicas del equipo. Puede, por ejemplo, impedir el acceso al escritorio del sistema y restringir parcialmente el uso del teclado y del ratón. La víctima puede interactuar únicamente con la ventana en la que se le exige el pago de un rescate. Las demás funciones del equipo quedan inutilizables. El ransomware de bloqueo tiene un lado positivo: por lo general, restringe el uso del equipo, pero deja sin cambios los archivos. La información de la víctima rara vez corre el riesgo de desaparecer.

b) **Ransomware de cifrado.** Este tipo de ransomware está diseñado para cifrarlos archivos más importantes de la víctima, como sus documentos, fotos y videos. El funcionamiento del equipo no se ve afectado en modo alguno. La víctima entra en pánico porque ve que sus archivos siguen allí, pero no puede abrirlos. Esta clase de malware muestra una leyenda en la que se exige el pago de un rescate y, por lo general, una cuenta regresiva. "Pague antes de que se agote el tiempo o perderá sus archivos", advierte el software. Como no todas las personas tienen copias de seguridad de sus archivos en la nube o en un soporte externo, el ransomware de cifrado puede tener un impacto muy profundo. No sorprende que muchas víctimas paguen para recuperar su información.

En el artículo de Checkpoint (2024), revela que, en los últimos seis meses, una empresa en Honduras ha sido blanco de aproximadamente 2,106 ataques semanales, con Darkgate como el malware más predominante en el país. Dentro de la lista de amenazas más comunes en el territorio hondureño, se identifican dos troyanos bancarios, un malware móvil (Necro), un ladrón de información (Lumma), una botnet (Darkgate) y un descargador de malware (Necro). Debido a esta actividad maliciosa, la divulgación de información se ha convertido en la vulnerabilidad más explotada, impactando al 84 % de las organizaciones en el país.



	Ransomware	Mobile	InfoStealer	Banking	Botnet
Honduras Avg.	1.1%	2.2%	3.3%	10.6%	13.9%
Latin Americas Avg.	5.4%	1.0%	11.0%	4.9%	12.7%

CHECK POINT

©2024 Check Point Software Technologies Ltd.

Figura 2 Porcentaje y comparación de Organizaciones afectadas por el malware semanalmente en Latam y Honduras.

Fuente: Checkpoint (2024).

2.1.1 ENTORNO ECONÓMICO

América Latina es una de las regiones con un desarrollo económico desigual, donde muchas empresas enfrentan limitaciones presupuestarias para invertir en ciberseguridad. La falta de recursos impacta la capacidad de implementar medidas preventivas avanzadas, dejando a muchas organizaciones en situación vulnerable ante ciberataques y pocas.

SOPHOS (2024), señala que la probabilidad de ser víctima de un ataque de ransomware tiende a incrementarse a medida que los ingresos de una organización son mayores. Las empresas que superan los USD 5,000 millones presentan la tasa más elevada de incidentes, alcanzando un 67 % de ataques registrados. No obstante, las compañías más pequeñas, con ingresos inferiores a USD 10 millones, también enfrentan un riesgo considerable, ya que cerca del 47 % de ellas experimentaron algún ataque de ransomware en el último año, lo que evidencia que ninguna organización está exenta de esta amenaza.

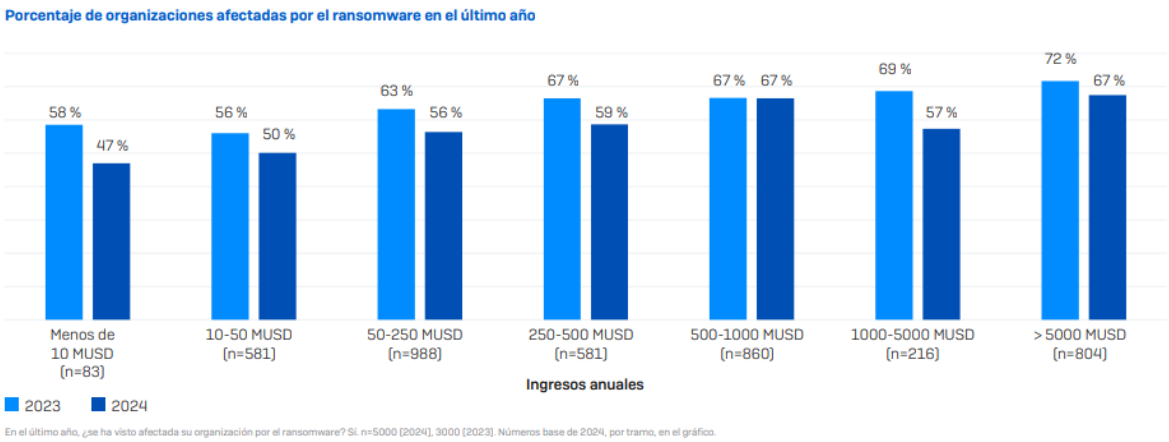


Figura 3 Porcentaje de Organizaciones afectadas por el ransomware en el último año.
Fuente: SOPHOS (2024).

En su libro, Barrios-Torres et al, (2022) indica que, la demanda de servicios de seguridad de la información experimentará un crecimiento significativo, superando los USD 455.9 millones. Para el año 2021, se proyecta que esta industria alcance un valor de USD 936.7 millones a nivel global, lo que representa un incremento del 15 % en comparación con 2019. Estas cifras reflejan la creciente importancia de la protección de datos y ciberseguridad en un entorno digital en constante evolución.

2.1.2 ENTORNO TECNOLÓGICO

La infraestructura tecnológica en América Latina es heterogénea; mientras algunos países

como Chile y Argentina tienen redes y sistemas más avanzados, en otros países el uso de software sin actualizaciones de seguridad es común. Esto, unido a la adopción acelerada de tecnologías sin medidas de protección adecuadas, crea un entorno favorable para el ransomware.

Para poder describir como nos afectan el malware en el entorno tecnológico, SOPHOS (2024) lo plantea así, de media, algo menos de la mitad (49 %) de los ordenadores de una organización se ven afectados por un ataque de ransomware. Sufrir el cifrado de todo el entorno es muy poco frecuente: solo el 4 % de las organizaciones señalaron que el 91 % o más de sus dispositivos habían sido alcanzados por un ataque. En el extremo opuesto, si bien algunos ataques afectan solo a un puñado de dispositivos, esto también es muy poco habitual. Según el informe, solo el 2 % de las organizaciones perjudicadas afirmaron que menos del 1 % de sus dispositivos habían sido atacados.

Para Gartner Inc (2024), en la actualidad, la mayoría de las decisiones sobre riesgos cibernéticos y las implementaciones se toman de forma distribuida, en los equipos de producto o las unidades de negocio, por medio de procesos ágiles, no de procesos en cascada controlados de forma centralizada y por etapas. Realizar cambios superficiales no será suficiente; los programas de ciberseguridad deben cambiar radicalmente.

Figura 4 Elementos de un Programa de Ciberseguridad.
Fuente: Gartner Inc, (2024).

2.1.3 ENTORNO SOCIAL

El nivel de educación y concienciación en ciberseguridad sigue siendo limitado en gran

parte de la región, lo que representa un desafío significativo para la protección de las organizaciones. En varios países, persiste una brecha en la capacitación del personal, lo que deja a las empresas vulnerables ante ataques cibernéticos. Esta falta de formación facilita la propagación de amenazas como el ransomware, especialmente a través de técnicas de ingeniería social, donde los atacantes explotan el desconocimiento de los empleados para acceder a sistemas críticos y comprometer la seguridad de la información.

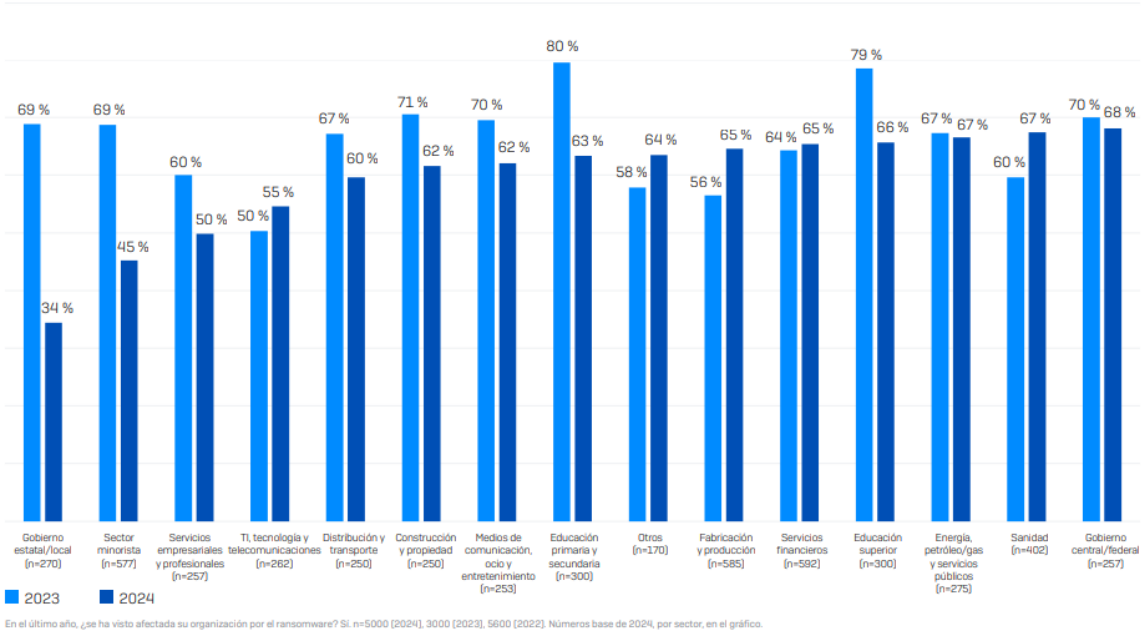


Figura 5 Elementos de un Programa de Ciberseguridad.
Fuente: SOPHOS (2024).

La ciberseguridad ha evolucionado hasta convertirse en un pilar esencial dentro del ámbito empresarial. Las amenazas cibernéticas, que antes eran consideradas exclusivamente un problema de TI, ahora representan un desafío estratégico que impacta directamente en la continuidad y el crecimiento de las organizaciones. Como resultado, las estrategias de seguridad han dejado de ser únicamente una responsabilidad técnica para integrarse en la gestión empresarial, con el objetivo de proteger los activos digitales y garantizar el cumplimiento de los objetivos estratégicos. En este contexto, la relación entre ciberseguridad y valor empresarial cobra cada vez más relevancia, ya que la protección de la información no solo resguarda la operación, sino que también fortalece la confianza y reputación corporativa (Deloitte Global, 2023).

Figura 6 La ciberseguridad genera valor en toda la empresa
Fuente: Contact Deloitte Global, (2023).

2.1.4 ENTORNO LEGAL

América Latina ha avanzado en la regulación de la ciberseguridad, pero de manera desigual. Países como México y Brasil han implementado leyes específicas para proteger los datos y regular la ciberseguridad, mientras que otros países aún no han adoptado normativas claras. La falta de legislación uniforme dificulta el desarrollo de un entorno seguro para las empresas.

Según Díaz (2022), en su informe de la Comisión Económica para América Latina (CEPAL) afirma que, en 2015, la UNODC, en el marco de la Comisión de Prevención del Delito y Justicia Penal (CCPCJ), lanzó el repositorio de delitos cibernéticos, una base de datos central de legislación, jurisprudencia y lecciones aprendidas sobre delitos cibernéticos y pruebas electrónicas. El repositorio de delitos informáticos tiene como objetivo ayudar a los países en sus esfuerzos por prevenir y enjuiciar eficazmente a los delincuentes cibernéticos. El repositorio consta de tres partes que tienen como objetivo facilitar los esfuerzos de los Estados contra el delito cibernético:

a) La Base de datos de legislación, que contiene legislación sustantiva y procesal sobre delitos cibernéticos y pruebas electrónicas de más de 180 países y se puede buscar por país, tipo de delito cibernético y aspectos procesales. La base de datos contiene extractos de leyes pertinentes a los delitos cibernéticos y cuestiones transversales y permite a los usuarios acceder a documentos legislativos completos;

b) La Base de datos de jurisprudencia, que contiene jurisprudencia y registros de operaciones

exitosas de aplicación de la ley, sobre delitos cibernéticos y delitos relacionados con pruebas electrónicas. Esto permite a los usuarios ver cómo los Estados abordan los casos de delitos cibernéticos tanto operativamente como en sus tribunales;

c) La base de datos de lecciones aprendidas, que contiene prácticas y estrategias nacionales para prevenir y combatir el delito cibernético. La información recopilada en esta base de datos se ha recopilado en el marco del Estudio integral de la UNODC sobre el delito cibernético y se complementa con estrategias nacionales de ciberdelincuencia y ciberseguridad.

2.2 MICROENTORNO

2.2.1 PERSPECTIVA CENTROAMERICANA

En Centroamérica, la ciberseguridad sigue siendo un desafío crítico para el sector público y privado. Según el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA) (2020), la falta de infraestructura tecnológica avanzada y la ausencia de regulaciones homogéneas han convertido a países como Guatemala, El Salvador y Nicaragua en objetivos frecuentes de ataques de ransomware, afectando la operatividad de instituciones gubernamentales y empresas privadas. En Costa Rica, el ataque del grupo Conti en 2022 paralizó varias instituciones gubernamentales y provocó pérdidas millonarias, evidenciando la falta de estrategias de respuesta eficaces en la región (BID, 2020).

En el Índice Global de Ciberseguridad (*Global Cybersecurity Index*, 2024) destaca que Centroamérica aún se encuentra rezagada en términos de madurez en ciberseguridad, con países como Panamá y Costa Rica liderando en la implementación de regulaciones y políticas de protección digital, mientras que Guatemala y Honduras presentan los mayores rezagos. La falta de un Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT) nacional en algunos países impide la coordinación efectiva ante ataques de gran escala, lo que deja a muchas empresas sin apoyo institucional.

En el sector empresarial, las brechas en ciberseguridad son evidentes. Mientras que bancos y empresas multinacionales en El Salvador, Costa Rica y Guatemala han adoptado normativas como ISO 27001 y NIST, la mayoría de pequeñas y medianas empresas (Pymes) aún carecen de planes de contingencia para enfrentar ataques de ransomware así lo plantea (ESET, 2023). En

comparación, países como México y Chile han avanzado en la regulación del sector financiero, exigiendo que sus instituciones adopten estándares internacionales obligatorios, algo que en Centroamérica sigue siendo opcional.

Otro problema clave es la falta de talento especializado. De acuerdo con el (BID, 2020), la región enfrenta una brecha significativa en educación en ciberseguridad. En Honduras, Guatemala y El Salvador, las universidades y empresas privadas han comenzado a ofrecer certificaciones y programas de formación, pero la demanda supera la oferta, lo que obliga a muchas empresas a contratar consultores externos. Panamá, en contraste, ha promovido iniciativas gubernamentales para capacitar talento local, alineándose con estrategias de ciberseguridad implementadas en países desarrollados.

2.2.2 PERSPECTIVA HONDUREÑA

Honduras ocupa la posición 178 a nivel mundial según el Índice Nacional de Seguridad Cibernética NCSI por sus siglas en inglés, lo que refleja un bajo nivel de desarrollo en términos de políticas de ciberseguridad, infraestructura de defensa y capacidad de análisis de ciberamenazas. Este contexto revela que el país carece de medidas efectivas y recursos suficientes para abordar las crecientes amenazas cibernéticas, lo que lo deja en una situación de alta vulnerabilidad frente a ataques como el ransomware. En el entorno empresarial hondureño, la situación es aún más crítica: la mayoría de las empresas, en particular las pequeñas y medianas, no cuentan con personal especializado ni con protocolos de respuesta bien establecidos, lo cual limita gravemente su capacidad de defensa y recuperación en caso de un ataque (NCSI, 2022).

Esta vulnerabilidad se agrava por la escasa inversión en tecnologías de protección y la falta de una cultura organizacional enfocada en la ciberseguridad. Muchos sistemas en estas empresas dependen de software y hardware obsoletos que son más susceptibles a intrusiones. Además, la falta de capacitación y concienciación entre los empleados sobre el manejo seguro de la información y los riesgos de ciberseguridad incrementa la probabilidad de incidentes.

En los datos que el Observatorio De La Ciberseguridad (2020) muestra, se explica que, en los últimos años, Honduras ha dado algunos pasos significativos hacia el fortalecimiento de su ciberseguridad a nivel institucional y legislativo, aunque persisten grandes desafíos en la implementación y en la protección integral de las empresas y organizaciones. El país ha puesto en marcha el proyecto de Ley Nacional de Ciberseguridad y Medidas de Protección ante los Actos de

Odio y Discriminación en Internet y Redes Sociales, el cual busca establecer una estrategia nacional de seguridad cibernética y un comité interinstitucional que supervise su desarrollo. Este proyecto refleja un creciente reconocimiento de la importancia de la ciberseguridad, aunque aún no cuenta con un CSIRT (Equipo de Respuesta a Incidentes de Seguridad Cibernética) nacional, lo que limita la capacidad de respuesta centralizada y coordinada ante ciberataques.

En 2016, Honduras estableció un acuerdo de cooperación con Israel con el propósito de fortalecer sus capacidades en prevención, defensa y respuesta ante ciberataques, enfocado principalmente en instituciones gubernamentales e infraestructuras críticas. Además, el país impulsa el programa "Transformación Digital para una Mayor Competitividad", una iniciativa financiada por el Banco Interamericano de Desarrollo (BID) y el gobierno hondureño, cuyo objetivo es modernizar la ciberseguridad a nivel nacional. Este programa busca mejorar la protección tanto en el sector público como en el privado, promoviendo estrategias más eficientes para enfrentar los crecientes desafíos en materia de seguridad digital (Observatorio De La Ciberseguridad, 2020).

A pesar de los avances en materia de seguridad cibernética, Honduras aún enfrenta deficiencias estructurales en la respuesta a incidentes, según el Observatorio De La Ciberseguridad (2020), aunque algunas empresas privadas han comenzado a ofrecer servicios especializados en gestión de incidentes, y las principales firmas del sector han implementado medidas para fortalecer su protección digital, la mayoría de las organizaciones siguen siendo altamente vulnerables. Esta fragilidad se debe, en gran parte, a la escasez de recursos especializados en ciberseguridad, lo que limita la capacidad del país para enfrentar eficazmente los crecientes riesgos cibernéticos.

El Observatorio De La Ciberseguridad (2020) destaca que, el gobierno hondureño ha implementado iniciativas para fortalecer la formación en ciberseguridad, incluyendo un acuerdo de cooperación con México en materia de ciberseguridad y ciberdefensa. Además, la Comisión Nacional de Telecomunicaciones (CONATEL) ha impulsado talleres y cursos básicos sobre seguridad informática. No obstante, la oferta de capacitación sigue siendo insuficiente, especialmente para la población en general y los empleados del sector privado, lo que representa un desafío significativo en la preparación de las empresas para enfrentar amenazas cibernéticas de manera efectiva.

También el Observatorio De La Ciberseguridad (2020) enfatiza que, en términos

legislativos, Honduras ha avanzado al revisar la Ley Nacional de Ciberseguridad. Sin embargo, aunque desde 2018 existe un anteproyecto de ley de protección de datos personales que contempla su aplicación tanto en el sector público como en el privado, este aún no ha sido aprobado, lo que representa una brecha importante en el marco normativo del país. Estos avances buscan proteger la privacidad de los usuarios y la información personal, lo cual es fundamental para la confianza en las tecnologías digitales. La agenda de Gobierno Digital, dentro de la Agenda Digital de Honduras 2014-2018, también busca modernizar la administración pública mediante la creación de una red gubernamental que centralice y proteja información crítica, lo cual es esencial para mejorar la transparencia y la eficacia en los servicios del sector público.

La escasez de personal especializado en ciberseguridad es un problema significativo para las empresas en Honduras, especialmente para las pequeñas y medianas empresas (pymes), que suelen tener menos recursos para contratar y retener expertos en el área. Esta carencia limita la capacidad de estas organizaciones para implementar medidas preventivas y responder adecuadamente ante un ataque de ransomware. Sin personal capacitado, las empresas no solo carecen de la supervisión continua necesaria para detectar intrusiones tempranas, sino también de la habilidad para llevar a cabo una recuperación rápida y eficaz en caso de incidente.

Los sistemas obsoletos son otro factor crítico. Es común ver empresas que sigan utilizando infraestructura tecnológica antigua, tanto en software como en hardware, que ya no recibe soporte técnico ni actualizaciones de seguridad. Este tipo de sistemas es más vulnerable a las brechas de seguridad, ya que los desarrolladores han dejado de proporcionar parches que corrigen vulnerabilidades. Esto facilita la explotación de fallos conocidos por parte de atacantes, aumentando así el riesgo de que se produzcan infecciones por ransomware.

Además, la falta de actualización tecnológica y capacitación en ciberseguridad está vinculada a una baja inversión en estos aspectos de mucha relevancia actual. En el contexto hondureño, la ciberseguridad suele ser vista como un gasto más que como una inversión esencial. Esto lleva a que muchas empresas ignoren o minimicen la importancia de protocolos de seguridad básicos, como los sistemas de respaldo y las políticas de actualización periódica. Sin estos elementos, las empresas carecen de una base sólida para defenderse de amenazas cibernéticas modernas y, cuando ocurre un ataque, están menos preparadas para restaurar sus operaciones de manera efectiva.

2.3 TEORÍAS DE SUSTENTO

2.3.1 MODELO DE CIBERSEGURIDAD EN PROFUNDIDAD

El modelo de Ciberseguridad en Profundidad (Defence in Depth) es una estrategia que incorpora múltiples capas de protección para reducir el riesgo de ciberataques, incluyendo el ransomware, según *Ransomware Defense-in-Depth* (2023), este enfoque abarca desde la infraestructura física hasta la gestión de la información, asegurando la implementación de medidas de prevención, detección y respuesta en toda la organización.

En Honduras, el ransomware se ha convertido en una amenaza crítica, ya que secuestra información clave y bloquea el acceso a sistemas esenciales. Aplicar el modelo de Ciberseguridad en Profundidad permite mitigar este riesgo al distribuir capas de seguridad en múltiples puntos de vulnerabilidad, incluyendo la red, el sistema operativo y las aplicaciones, proporcionando así una protección integral contra este tipo de ataques. Dentro de las prácticas y tecnologías utilizadas en este modelo destacan:

- **Autenticación multifactor**: Asegura que sólo los usuarios autorizados tengan acceso a información y sistemas sensibles, limitando así los puntos de acceso para posibles atacantes
- **Segmentación de redes**: Divide la red de una empresa en subredes, limitando la propagación del ransomware y protegiendo la información crítica de la empresa en caso de una infección.
- **Respaldo y recuperación de datos**: Establece un sistema de copias de seguridad automatizadas que protege los datos frente a los ataques de ransomware, permitiendo restaurarlos sin tener que ceder ante las demandas de los atacantes

En el contexto empresarial de Honduras, se describe que el modelo de Ciberseguridad en profundidad debería ser particularmente relevante, ya que se necesita lo siguiente:

- **Reducir el impacto de los ataques de ransomware**: Al aplicar múltiples niveles de protección, este modelo minimiza la probabilidad de que un ataque tenga éxito en secuestrar información crítica.
- **Facilitar la respuesta ante incidentes**: Al implementar herramientas de monitoreo y detección temprana, las organizaciones pueden identificar posibles amenazas antes de que estas se propaguen.

- **Mejorar la resistencia organizacional**: Este enfoque permite que las empresas mantengan la continuidad de sus operaciones, incluso si algunas de sus capas de seguridad son comprometidas.

El modelo de Ciberseguridad en Profundidad se presenta como una estrategia fundamental para mitigar el impacto del ransomware en las empresas hondureñas, especialmente aquellas con recursos limitados. Este enfoque se basa en la implementación de múltiples capas de seguridad, incluyendo autenticación multifactor, segmentación de redes y copias de seguridad, lo que permite contener la propagación del malware, minimizar daños y recuperar la información sin necesidad de pagar un rescate. Su carácter escalable y flexible facilita su adopción progresiva, haciéndolo una solución viable para organizaciones con presupuestos ajustados, al proporcionar un marco de defensa adaptable a sus capacidades (*Ransomware Defense-in-Depth*, 2023).

2.3.2 INTELIGENCIA DE AMENAZAS Y RESPUESTA PROACTIVA

La Inteligencia de Amenazas (Threat Intelligence) consiste en la recopilación y análisis de información sobre amenazas cibernéticas, con el objetivo de identificar patrones, tácticas y posibles atacantes. Esta estrategia resulta esencial para prevenir y mitigar ataques de ransomware, ya que permite detectar indicios de actividad maliciosa y aplicar medidas proactivas para neutralizar posibles riesgos antes de que afecten a una organización.

La Inteligencia de Amenazas es especialmente útil para las empresas en Honduras, ya que:

- **Permite el análisis preventivo de amenazas**: Mediante la recopilación de información sobre ciberataques previos, se pueden prever nuevas tácticas de ataque y establecer medidas de protección adaptadas a las necesidades del contexto local.
- **Mejora la toma de decisiones en ciberseguridad**: El análisis de amenazas previas ayuda a los equipos de ciberseguridad a tomar decisiones informadas sobre las mejores prácticas y las tecnologías de defensa más adecuadas.
- **Optimiza los recursos de defensa**: Al enfocar los recursos en amenazas específicas, las organizaciones pueden mejorar la eficacia de sus defensas sin incurrir en gastos excesivos.

La Inteligencia de Amenazas ayuda a las empresas hondureñas a anticipar y mitigar los ataques de ransomware mediante la identificación de tácticas comunes. Al enfocarse en amenazas específicas del contexto local, este modelo optimiza los recursos al priorizar las medidas más

críticas y rentables. También permite una respuesta proactiva y acelera la detección de ataques, lo cual es esencial en un entorno donde los recursos y la disponibilidad de servicios de ciberseguridad pueden ser limitados. Además, facilita una mejor capacitación y toma de decisiones informadas en materia de seguridad (*Ransomware Defense-in-Depth*, 2023).

2.4 METODOLOGÍAS TEMÁTICAS

La investigación adoptará un enfoque cualitativo para abordar los objetivos de estudio, con un enfoque específico en la aplicación de metodologías de **análisis de riesgos** y **desarrollo de planes de contingencia**.

2.4.1 ANÁLISIS DE RIESGOS

Esta metodología se centra en identificar, evaluar y priorizar los riesgos que enfrenta una organización en términos de ciberseguridad, especialmente en el contexto de ataques de tipo ransomware. Se justifica su uso dado que permite analizar los puntos débiles en la infraestructura tecnológica y en las prácticas de seguridad actuales, fundamentales para el objetivo de mejorar la respuesta ante ataques cibernéticos.

2.4.2 METODOLOGÍA PARA EL DESARROLLO DE PLANES DE CONTINGENCIA

Para la creación del plan de contingencia, se empleará una metodología estructurada que combina los lineamientos de la norma ISO 22301, orientada a la gestión de la continuidad del negocio, y la norma ISO 27001, enfocada en la gestión de la seguridad de la información, que según Sotres Cruz (2012), la ISO 22301 es una norma internacional que establece los requisitos para los Sistemas de Gestión de la Continuidad del Negocio (SGCN). Su propósito es ayudar a las organizaciones a prevenir, prepararse, responder y recuperarse ante situaciones imprevistas, como desastres naturales, ciberataques, pandemias o conflictos armados. Esta norma proporciona un marco estructurado para garantizar la continuidad operativa y la gestión eficaz de incidentes, permitiendo a las empresas mantener sus funciones críticas y minimizar el impacto de interrupciones en sus actividades.

Para UNIR (2019), la ISO 27001 es una norma internacional de Seguridad de la Información diseñada para garantizar la confidencialidad, integridad y disponibilidad de los datos dentro de una organización, así como de los sistemas y aplicaciones que los gestionan. Su enfoque es genérico y adaptable, permitiendo su implementación independientemente del entorno,

contexto, activos tecnológicos o cultura organizacional. Esta norma establece un marco de referencia que facilita la identificación y gestión de riesgos de seguridad de la información, proporcionando metodologías reconocidas a nivel internacional. Su flexibilidad permite que sea aplicada en diversos sectores empresariales, asegurando una protección eficaz frente a amenazas cibernéticas y fortaleciendo la resiliencia organizacional.

De acuerdo con Sotres Cruz (2012), un Sistema de Gestión de la Continuidad del Negocio (BCMS, por sus siglas en inglés) permite a las organizaciones evaluar continuamente los riesgos y conocer su grado de preparación para enfrentar situaciones inesperadas, minimizando el impacto de posibles interrupciones en sus operaciones. En este sentido, se define como un "proceso de gestión holístico que identifica las amenazas potenciales para una organización y los efectos que podrían generar en sus operaciones si estas se materializan. Además, establece un marco de trabajo para fortalecer la resiliencia organizacional, garantizando una respuesta efectiva y la protección de los intereses clave, la reputación, la imagen de marca y las actividades de valor añadido".

Según UNIR (2019), la capacidad de respuesta organizacional ante eventos catastróficos que afecten la continuidad de productos y servicios puede fortalecerse a través de la implementación de Planes de Continuidad del Negocio (BCP, por sus siglas en inglés). Estos planes tienen como prioridad salvaguardar el bienestar del personal, seguido por la rentabilidad económica, la imagen, la reputación y las actividades de creación de valor de la organización. En este contexto, la ISO 27001 se fundamenta en el ciclo de gestión de calidad PDCA (Plan-Do-Check-Act), también conocido como ciclo de Deming, proporcionando una estructura metodológica para la gestión efectiva de la seguridad de la información y la continuidad operativa.

- Planificar (“Plan”): etapa inicial de diseño del SGSI en la que se realiza la identificación inicial de los riesgos asociados con la Seguridad de la información. Esta cuestión se complementa con un análisis cualitativo y cuantitativo (si es necesario) de los riesgos identificados y la planificación de la respuesta y los controles necesarios para la mitigación de estos.
- Hacer (“Do”): implantación y operación del Sistema de Gestión de Seguridad de la Información definido y desarrollado.
- Verificar (“Check”): revisar y evaluar su eficacia y eficiencia. Si el desempeño no es el esperado analizar las causas y determinar las mejoras.

- Actuar (“Act”): mejora continua del SGSI.

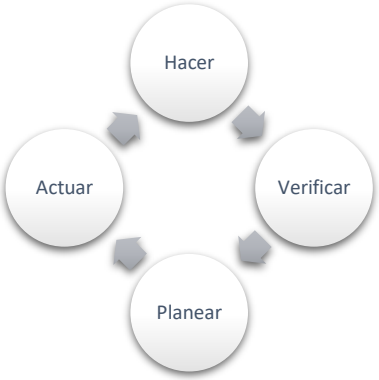


Figura 7 El Círculo de Deming (Shewhart): Ciclo PDCA (PHVA)
Fuente: Elaboración propia basado en el círculo de Deming.

Adicionalmente, emplearemos la metodología **Scrum**, como lo indica Sachdeva (2016) en su artículo, debido a que es un marco de trabajo ágil que permite a las personas abordar problemas complejos y adaptativos, al mismo tiempo que entregan productos de manera eficiente y creativa con el máximo valor. Scrum proporciona un plan de valores, roles y pautas para ayudar al equipo a concentrarse en la iteración y la mejora continua en proyectos complejos, como lo es el desarrollo de un plan de contingencia y respuesta eficaz ante ciberataques de tipo ransomware en empresas hondureñas. Por otro lado, Scrum se basa en equipos pequeños multidisciplinarios que trabajan en ciclos iterativos centrados en el cliente, creando un producto de forma incremental.

Y afirmando el artículo de Sachdeva (2016), Scrum se concibe como una herramienta o marco de trabajo adaptable para la creación de productos complejos. Se distingue por su flexibilidad en el desarrollo de productos, sin imponer prácticas específicas en áreas como ingeniería, gestión de personas, riesgos u otras. Esta ausencia de prescripciones en ingeniería permite, y a menudo aconseja, la integración de prácticas externas a Scrum que puedan potenciar su eficacia.

2.5 HERRAMIENTAS

2.5.1 HERRAMIENTAS OFIMÁTICAS

Tabla 1 Herramientas Ofimáticas

Herramienta	Descripción	Ventajas	Desventajas	Costo	URL
Microsoft 365	Suite completa de	Almacenamie	Costo mensual,	A partir de	https://www.mic

Herramienta	Descripción	Ventajas	Desventajas	Costo	URL
	aplicaciones (Word, Excel, PowerPoint, etc.)	nto en la nube e integración con otros servicios.	requiere conexión a internet para algunas funciones.	$6.99/mes	rosoft.com/es-es/microsoft-365/
Google Workspace Individual	Suite de productividad en la nube con aplicaciones como Docs, Sheets y Slides. Ofrece colaboración en tiempo real y almacenamiento gratuito.	Gratuito en su versión básica, colaboración en tiempo real, integración con otros servicios de Google.	Funcionalidades más limitadas en la versión gratuita, dependencia de la conexión a internet.	Gratis (básico), planes pagos disponibles	https://workspace.google.com/
LibreOffice	Suite ofimática de código abierto y gratuita, compatible con formatos de Microsoft.	Completamente gratuita, amplia gama de funciones, personalizable.	Interfaz menos intuitiva que otras opciones, puede carecer de algunas características avanzadas.	Gratis	https://www.libreoffice.org/

Fuente: Elaboración propia

Para optimizar la elaboración y recopilación de información en este proyecto, se ha seleccionado Microsoft 365 como suite ofimática principal. Esta elección se fundamenta en la necesidad de contar con una plataforma integrada que facilite la colaboración entre el equipo, la gestión de documentos y la accesibilidad a la información desde cualquier dispositivo.

2.5.2 HERRAMIENTAS DE PLANIFICACIÓN

Tabla 2 Herramientas de Planificación

Herramienta	Descripción	Ventajas	Desventajas	Costo	URL
Trello	Tablero visual para organizar tareas y proyectos.	Fácil de usar, intuitiva, gratuita, flexible.	Limitada para proyectos complejos, pocas opciones de personalización.	Gratis (plan básico), planes pagos disponibles	https://trello.com/
Asana	Plataforma de gestión de proyectos y tareas.	Amplias opciones de personalización, colaboración en tiempo real, integración con otras herramientas.	Curva de aprendizaje algo más pronunciada, interfaz puede resultar compleja.	Gratis (plan básico), planes pagos disponibles	https://asana.com/

Herramienta	Descripción	Ventajas	Desventajas	Costo	URL
Jira	Herramienta de gestión de proyectos ágiles.	Muy potente para equipos de desarrollo, gran cantidad de funcionalidades.	Compleja para usuarios no técnicos, costo elevado para pequeñas empresas.	Desde $10/usuario/mes	https://www.atlassian.com/software/jira

Fuente: Elaboración propia

Para la planificación se ha seleccionado Trello como la plataforma de colaboración y gestión de tareas para este proyecto debido a su alta flexibilidad. Permite adaptar los tableros y las tarjetas a las necesidades específicas de cada equipo y proyecto, facilitando la organización y el seguimiento del trabajo.

2.5.3 HERRAMIENTAS DE MENSAJERÍA INSTANTÁNEA

Tabla 3 Herramientas de Mensajería Instantánea

Herramienta	Descripción	Ventajas	Desventajas	Costo	URL
WhatsApp	Plataforma de mensajería instantánea para comunicación personal y grupos pequeños.	Fácil de usar, cifrado de extremo a extremo (mensajes individuales), amplia base de usuarios.	Limitaciones en grupos grandes, funcionalidades básicas.	Gratuito (con publicidad en algunos países)	https://www.whatsapp.com/
Telegram	Plataforma de mensajería con enfoque en privacidad y funcionalidades avanzadas.	Cifrado de extremo a extremo, canales temáticos, bots.	Interfaz puede resultar compleja para algunos usuarios.	Gratuito (con opciones de pago para funciones adicionales)	https://telegram.org/
Slack	Plataforma de colaboración en equipos, diseñada para comunicación laboral.	Integración con diversas herramientas, canales organizados por proyectos, búsqueda avanzada.	Curva de aprendizaje algo más pronunciada, costo puede ser elevado para equipos pequeños.	Planes gratuitos y de pago con diferentes funcionalidades	https://slack.com/

Fuente: Elaboración propia

WhatsApp ha sido seleccionado como herramienta de mensajería instantánea debido a su amplia adopción y familiaridad entre los usuarios. Actualmente ya se utiliza esta aplicación de forma regular, facilitando así la comunicación y la gestión de tareas y reuniones.

2.5.4 HERRAMIENTAS DE REUNIONES Y VIDEO LLAMADAS

Tabla 4 Herramientas de Reuniones y Video llamadas

Herramienta	Descripción	Ventajas	Desventajas	Costo	URL
Google Meet	Plataforma de videoconferencias integrada en Google Workspace, ideal para equipos que utilizan otros productos de Google.	Fácil de usar, alta calidad de video y audio, integración con otras herramientas de Google, gratuito para uso personal.	Limitaciones en el número de participantes en el plan gratuito, menos funciones avanzadas que Zoom.	Gratuito para uso personal; planes de pago para empresas.	meet.google.com
Zoom	Plataforma de videoconferencia muy popular, conocida por su facilidad de uso y estabilidad.	Amplias opciones de personalización, gran cantidad de participantes, grabación de reuniones, chat integrado.	Interfaz puede resultar abrumadora para nuevos usuarios, ha tenido problemas de seguridad en el pasado.	Gratuito para reuniones de hasta 40 minutos; planes de pago para más funcionalidades.	zoom.us
Microsoft Teams	Plataforma de colaboración que incluye videoconferencias, chat, almacenamiento en la nube y otras herramientas integrada con Microsoft 365.	integración con otras aplicaciones de Microsoft, adecuada para equipos que utilizan Microsoft 365.	Puede resultar compleja para usuarios que no están familiarizados con el ecosistema de Microsoft,	Gratuito para uso personal con funcionalidades limitadas; planes de pago para empresas.	https://www.microsoft.com/es-cl/microsoft-teams/download-app

Fuente: Elaboración propia

Para facilitar la comunicación y colaboración en tiempo real, se ha seleccionado Google Meet como herramienta principal para reuniones y video llamadas.

2.5.5 HERRAMIENTAS DE ANÁLISIS Y VISUALIZACIÓN DE DATOS

Tabla 5 Herramientas de Análisis de Datos

Herramienta	Descripción	Ventajas	Desventajas	Costo	URL
Power BI	Plataforma de BI Microsoft para visualizar y analizar datos de forma interactiva.	Interfaz intuitiva, integra con otras herramientas de	curva de aprendizaje algo pronunciada para usuarios sin experiencia en BI.	Limitaciones en versión gratuita, planes de pago para empresas.	powerbi.microsoft.com

Herramienta	Descripción	Ventajas	Desventajas	Costo	URL
SPSS	Software estadístico especializado en análisis de datos complejos.	Potente para análisis estadísticos avanzados, interfaz familiar para usuarios acostumbrados a software estadístico.	Interfaz menos intuitiva que Power BI, costo elevado de las licencias, puede resultar lento para grandes conjuntos de datos.	Licencias de pago con diferentes niveles de funcionalidad.	https://www.ibm.com/es-es/products/spss-statistics
Python	Lenguaje de programación versátil utilizado para una amplia gama de tareas, incluyendo análisis de datos.	Flexibilidad, amplia comunidad y librerías (Pandas, NumPy, MatplotLib), código abierto y gratuito.	Curva de aprendizaje más pronunciada, puede ser más complejo para usuarios sin experiencia en programación.	Gratuito.	python.org

Fuente: Elaboración propia

Con el objetivo de transformar los datos en información relevante, se ha elegido Python como herramienta principal de análisis y visualización de datos, debido a su flexibilidad, potencia y amplia gama de bibliotecas especializadas como Pandas, NumPy y Matplotlib, que permiten realizar análisis profundos y visualizaciones claras, adecuadas para la interpretación de resultados en el contexto de la ciberseguridad y ransomware.

2.6 CONCEPTUALIZACIÓN

Amenaza

Una amenaza se define como cualquier circunstancia o evento que posee la capacidad de explotar vulnerabilidades y generar impactos negativos en diversos ámbitos. Estos impactos pueden afectar las operaciones de una organización, sus activos (incluyendo información y sistemas), individuos, otras organizaciones o incluso la sociedad en su conjunto. Las amenazas pueden manifestarse de diversas formas, ya sea a través de individuos o grupos, entidades como organizaciones o naciones, acciones específicas o sucesos inesperados. En la actualidad, el ransomware emerge como una amenaza particularmente relevante y preocupante (NICCS, 2024).

Ciberseguridad

La ciberseguridad se concibe como un conjunto integrado de prácticas, tecnologías y procesos cuyo objetivo principal es la protección de redes, dispositivos, programas y datos frente a ataques, daños o accesos no autorizados. De acuerdo con el Instituto Nacional de Estándares y

Tecnología (NIST, por sus siglas en inglés), la ciberseguridad abarca la capacidad de proteger o defender el uso del ciberespacio contra ataques cibernéticos (NIST, 2023).

Confidencialidad

Una propiedad según la cual la información no se divulga a los usuarios, procesos o dispositivos a menos que hayan sido autorizados para acceder a ella. Preservar las restricciones autorizadas sobre el acceso y la divulgación de información, incluidos los medios para proteger la privacidad personal y la información confidencial (NICCS, 2024).

Criptomoneda

Moneda digital en la que las transacciones son verificadas y los registros mantenidos por un sistema descentralizado que utiliza criptografía, en lugar de una autoridad centralizada. Al no están reguladas ni controladas por ninguna institución y no requieren de intermediaros en las transacciones. Se usa una base de datos descentralizada, *blockchain* o registro contable compartido, para el control de estas transacciones (NICCS, 2024).

Criptografía

Un procedimiento computacional definido que toma entradas variables, incluida una clave criptográfica, y produce una salida, además el uso de técnicas matemáticas para proporcionar servicios de seguridad, como confidencialidad, integridad, autenticación de entidades y autenticación del origen de los datos. El arte o la ciencia relativa a los principios, medios y métodos para convertir texto simple en texto cifrado y para restaurar texto cifrado en texto simple (NICCS, 2024).

End-Point Protección

(Plataforma de protección de puntos finales), son medidas de seguridad implementadas a través de software para proteger las máquinas de los usuarios finales, como estaciones de trabajo y computadoras portátiles, contra ataques, por ejemplo, antivirus, antispyware, antiadware, firewalls personales, sistemas de detección y prevención de intrusiones basados en host (Johnson et al, 2019).

Gestión de incidentes

Las actividades que abordan los efectos directos a corto plazo de un incidente y que

también pueden apoyar la recuperación a corto plazo. En el marco de la fuerza laboral, el trabajo de ciberseguridad consiste en que una persona: Responde a situaciones de crisis o urgentes dentro del dominio pertinente para mitigar amenazas inmediatas y potenciales; utiliza enfoques de mitigación, preparación, respuesta y recuperación, según sea necesario, para maximizar la supervivencia de la vida, la preservación de la propiedad y la seguridad de la información. Investiga y analiza todas las actividades de respuesta pertinentes (NICCS, 2024).

Infraestructura Crítica

Los sistemas y activos, tanto físicos como virtuales, son fundamentales para el funcionamiento de la sociedad. Su incapacidad, interrupción o destrucción podría generar un impacto significativo en diversas áreas críticas, como la seguridad nacional, la estabilidad económica, la salud pública y el medio ambiente. La alteración de estos recursos esenciales no solo compromete la continuidad operativa de sectores estratégicos, sino que también puede desencadenar efectos en cascada que afecten el bienestar social y la infraestructura de un país (NICCS, 2024).

Informática forense digital

El proceso de identificar, analizar, evaluar y comunicar el riesgo y aceptarlo, evitarlo, transferirlo o controlarlo a un nivel aceptable considerando los costos y beneficios asociados de cualquier acción adoptada (NICCS, 2024).

1. Realizar una evaluación de riesgos;
2. Implementar estrategias para mitigar los riesgos;
3. Monitoreo continuo del riesgo a lo largo del tiempo;
4. Documentar el programa general de gestión de riesgos.

Ingeniería social

El uso del engaño para manipular a individuos para que divulguen información confidencial o personal que pueda usarse con fines fraudulentos, como que revelen información confidencial o realicen acciones que pongan en riesgo su seguridad. En el ámbito de la ciberdelincuencia, la ingeniería social es una táctica que se basa en explotar las vulnerabilidades humanas de las personas, en lugar de las técnicas (NICCS, 2024).

Plan de Contingencia

Un plan de contingencia es un conjunto de estrategias y procedimientos establecidos por una organización para responder a eventos imprevistos que puedan interrumpir sus operaciones normales. Según la norma ISO 22301, “un plan de contingencia es una parte esencial de la continuidad del negocio que asegura que la organización esté preparada para responder a interrupciones de manera eficaz” (Sotres Cruz, 2012).

Ransomware

Es una clase de malware que representa un riesgo para ti y para tu dispositivo, el término con el que comienza, “ransom”, es una palabra inglesa que significa “rescate”. El ransomware es un software extorsivo: su finalidad es impedirte usar tu dispositivo hasta que hayas pagado un rescate. Normalmente, una infección con ransomware ocurre del siguiente modo. Para empezar, el ransomware se introduce en el dispositivo. A continuación, dependiendo del tipo de ransomware, se cifra por completo el sistema operativo o solo algunos de los archivos. Finalmente, se le exige a la víctima el pago de un rescate (AO Kaspersky Lab, 2024).

Vulnerabilidad

Una debilidad característica o específica que hace que una organización o un activo (como la información o un sistema de información) quede expuesto a la explotación por una amenaza determinada o sea susceptible a un peligro determinado. Característica de la ubicación o la postura de seguridad o del diseño, los procedimientos de seguridad, los controles internos o la implementación de cualquiera de estos que permiten que se produzca una amenaza o un peligro (NICCS, 2024).

2.7 MARCO LEGAL

2.7.1 MARCO LEGAL INTERNACIONAL

En un contexto global donde los ciberataques, como el ransomware, representan una amenaza creciente para las empresas y organizaciones, es fundamental analizar las disposiciones legales existentes que buscan mitigar sus impactos. Los marcos legales internacionales establecen lineamientos y obligaciones para prevenir, gestionar y responder a incidentes cibernéticos, promoviendo la protección de datos sensibles y la resiliencia de los sistemas de información.

Este apartado explora la normativa internacional más relevante, con un enfoque particular

en las legislaciones de Estados Unidos y Europa, que sirven como referencia en la lucha contra el cibercrimen. Estas regulaciones no solo abordan aspectos de seguridad, sino también mecanismos de cooperación internacional y pautas para la notificación de incidentes, elementos esenciales para enfrentar el desafío del ransomware en un entorno cada vez más digitalizado.

Tabla 6 Legislación Internacional

Ley	Año	Descripción
Estrategia Nacional De Ciberseguridad de Estados Unidos	2023	Marco estratégico de EE.UU. que establece los lineamientos y acciones para proteger la infraestructura crítica, sistemas y datos del país de ciberataques. Coordina esfuerzos gubernamentales, privados y de la sociedad civil.
Ley de Privacidad del Consumidor de California (CCPA)	2020	Ley estadounidense que otorga a los residentes de California ciertos derechos sobre sus datos personales, como el derecho a conocer qué información se recopila, el derecho a solicitar la eliminación de datos y el derecho a optar por no vender datos personales.
Reglamento General de Protección de Datos (GDPR)	2018	Ley europea que establece un marco común para la protección de datos personales de los ciudadanos de la UE. Define los derechos de los individuos sobre sus datos y las obligaciones de las organizaciones que los procesan.
NIST	2024	Conjunto de publicaciones del Instituto Nacional de Estándares y Tecnología de los EEUU que proporcionan guías para la seguridad cibernética.
ISO 27001	2022	Norma internacional que establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI).
ITIL	2019	Conjunto de mejores prácticas para la gestión de servicios de TI, que ayuda a las organizaciones a alinear los servicios de TI con los objetivos del negocio
COBIT	2019	Marco de referencia para la gobernanza y gestión de TI, que ayuda a las organizaciones a asegurar que la información esté disponible, confidencial y completa, para apoyar los objetivos del negocio.

Fuente: Elaboración Propia

Si bien las legislaciones internacionales como el **GDPR** y la **Estrategia Nacional de Ciberseguridad de EE. UU.** ofrecen lineamientos avanzados para abordar amenazas cibernéticas, su implementación en el contexto nacional de Honduras presenta desafíos significativos. Por ejemplo:

- **Transferencia de marcos internacionales:** Aunque las normativas internacionales

promueven la cooperación y la estandarización, su aplicabilidad depende de la capacidad de los países para adaptarlas a sus propios sistemas legales y contextos socioeconómicos. En Honduras, la falta de infraestructura tecnológica robusta y la limitada formación en ciberseguridad dificultan la adopción de estas normativas.

- **Relevancia para la región:** Aunque las regulaciones internacionales enfatizan la cooperación transnacional, su impacto directo en el país es limitado debido a la escasa participación de Honduras en iniciativas regionales de ciberseguridad. Esto subraya la necesidad de fortalecer marcos legales locales que se alineen con los estándares globales.

2.7.2 MARCO LEGAL NACIONAL

En Honduras, el avance de las tecnologías digitales ha traído consigo nuevos desafíos en el ámbito de la ciberseguridad, siendo el ransomware una de las amenazas más graves para empresas y organizaciones. Ante este panorama, el marco legal nacional desempeña un papel crucial al establecer las bases para la prevención, detección y respuesta ante incidentes cibernéticos. Sin embargo, el país enfrenta una importante limitación: la ausencia de una estrategia nacional de ciberseguridad que permita coordinar y fortalecer las acciones en este ámbito.

Este apartado examina las principales normativas hondureñas relacionadas con la protección de datos, la seguridad de la información y los delitos informáticos, tales como el código penal, y las normas del CONSUCOOP Y CNBS. Estas legislaciones buscan garantizar la seguridad de los sistemas tecnológicos y proteger los derechos de las personas y las operaciones críticas frente a ataques como el ransomware, aunque su alcance se ve limitado por la falta de un enfoque estratégico integral.

Tabla 7 Legislación de Honduras

Ley	Año	Descripción
Constitución de la Republica de Honduras	1982	Establece los fundamentos del orden jurídico hondureño, garantizando derechos como el honor, la intimidad personal, familiar y a la propia imagen.
Código Penal de Honduras (Decreto No. 130-2017**)**	2019	Contiene diversas disposiciones penales que protegen la privacidad y los datos personales, tipificando delitos como la interceptación de comunicaciones, el acceso no autorizado a sistemas informáticos, la usurpación de identidad y la divulgación de información privada.
Normas para Regular la	2005	Estas normas, emitidas por la Comisión Nacional de Bancos y

Ley	Año	Descripción
Administración de las Tecnologías de la Información y Comunicaciones en las Instituciones del Sistema Financiero		Seguros (CNBS), establecen los requisitos mínimos de seguridad para la protección de la información en las instituciones financieras, incluyendo medidas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales de los clientes.
Norma para la Administración de Tecnologías de la Información y Comunicaciones para las Cooperativas de Ahorro y Crédito	2023	Similar a la norma anterior, pero dirigida específicamente a las cooperativas de ahorro y crédito. Establece los estándares técnicos y de seguridad que deben cumplir estas entidades para proteger la información de sus asociados.

Fuente: Elaboración propia

Desafíos presentes en la legislación hondureña

- **Alcance limitado de las normativas:** Aunque existen disposiciones legales relevantes en el Código Penal y regulaciones específicas para sectores financieros y cooperativas, estas normativas no abordan de manera integral las amenazas avanzadas como el ransomware. Por ejemplo, la **Norma de Administración de Tecnologías de la Información para Cooperativas de Ahorro y Crédito** establece requisitos técnicos básicos, pero carece de lineamientos específicos para la gestión de incidentes cibernéticos complejos.
- **Ausencia de una estrategia nacional:** La falta de un marco estratégico coordinado debilita la capacidad del país para responder a ciberataques. Esto afecta la implementación de medidas preventivas, la notificación de incidentes y la cooperación con entidades internacionales, limitando la resiliencia frente al ransomware.
- **Impacto en el contexto local:** Aunque las normas de la CNBS y CONSUCOOP son fundamentales para sectores específicos, no tienen un alcance nacional generalizado. Esto deja a muchas empresas fuera de un marco regulatorio robusto, exponiéndolas a mayores riesgos.

CAPÍTULO III – METODOLOGÍA DE LA INVESTIGACIÓN

La metodología constituye un componente fundamental de cualquier proceso de investigación, ya que proporciona las directrices necesarias para llevar a cabo el estudio de manera sistemática y estructurada. Este capítulo detalla el enfoque metodológico adoptado, así como las técnicas y herramientas utilizadas para alcanzar los objetivos planteados. En el caso de esta investigación, cuyo propósito es desarrollar un plan de contingencia y respuesta eficaz ante ciberataques de tipo ransomware en empresas hondureñas, se emplea un diseño mixto que integra enfoques cualitativos y cuantitativos para garantizar un análisis integral del problema (Roberto Hernández Sampieri, 2014).

Se justifica el uso de esta metodología por su capacidad para abordar tanto los aspectos descriptivos como los explicativos del fenómeno estudiado, permitiendo no solo identificar las vulnerabilidades existentes en las empresas hondureñas, sino también diseñar soluciones prácticas basadas en estándares internacionales como las normas ISO 22301 e ISO 27001 (Sotres Cruz, 2012; UNIR, 2019) además, se describen los criterios de selección de la muestra, las técnicas de recolección de datos y los procedimientos empleados, asegurando la validez y confiabilidad de los resultados obtenidos.

En este capítulo también se detalla el marco conceptual y operativo que sustenta la investigación, proporcionando claridad sobre los términos y definiciones clave que estructuran el estudio. De esta manera, se busca establecer una base sólida para responder de manera efectiva a los objetivos y preguntas de investigación planteadas, ofreciendo un modelo de gestión adaptable y efectivo frente a las amenazas del ransomware en el contexto empresarial de Honduras.

3.1 ENFOQUE

El enfoque de la presente investigación es **cualitativo**, lo que implica un proceso dinámico, flexible e interpretativo para comprender el fenómeno del ransomware en empresas hondureñas. De acuerdo con Roberto Hernández Sampieri (2014), este enfoque se fundamenta en la exploración profunda de experiencias, percepciones y significados atribuidos por los actores involucrados, permitiendo reconstruir su realidad desde una perspectiva holística.

A diferencia del enfoque cuantitativo, donde las preguntas e hipótesis suelen estar definidas desde el inicio, el enfoque cualitativo permite formular, ajustar y perfeccionar las preguntas de

investigación a lo largo del proceso, en función de los datos recolectados y analizados. Este proceso es **circular** y permite regresar a etapas previas cuando es necesario, lo que asegura una comprensión más contextualizada y detallada del problema investigado (Roberto Hernández Sampieri, 2014).

Justificaciones para la elección del enfoque cualitativo:

1. **Naturaleza exploratoria del fenómeno:** El ransomware afecta a las empresas de múltiples maneras técnicas, organizacionales y humanas. Este enfoque permite analizar las estrategias de respuesta, percepciones sobre el riesgo y barreras contextuales desde el punto de vista de los participantes.
2. **Contexto local único:** En Honduras, la falta de una estrategia nacional de ciberseguridad y la infraestructura limitada hacen que las experiencias de las empresas sean distintas a las de otros países. La investigación cualitativa es ideal para captar las particularidades de este entorno.
3. **Proceso inductivo:** Partiendo de las observaciones y datos recolectados (a través de entrevistas, revisión documental y análisis de casos), se busca construir una teoría que represente fielmente las dinámicas de las empresas frente a los ataques de ransomware.

Características clave del enfoque cualitativo aplicado:

- **Métodos no estandarizados:** Se emplearán técnicas como entrevistas abiertas, revisión de documentos y análisis de historias de vida, permitiendo capturar las vivencias y significados desde la perspectiva de los participantes.
- **Adaptabilidad:** El diseño de la investigación podrá ajustarse según las necesidades emergentes del estudio, ya sea al identificar nuevos informantes clave o al incorporar datos no previstos inicialmente.
- **Interpretación del significado:** Más allá de registrar hechos objetivos, se analizarán las interacciones, emociones y subjetividades de los participantes, ofreciendo un entendimiento más profundo y empático del problema.
- **Perspectiva naturalista:** La investigación se llevará a cabo en los contextos reales de las empresas, evitando la manipulación de variables y respetando las dinámicas naturales de los actores involucrados.

3.2 ALCANCE

El alcance de esta investigación es descriptivo, ya que busca documentar las principales vulnerabilidades y factores de riesgo que enfrentan las empresas hondureñas frente a ataques de tipo ransomware. A través de un enfoque cualitativo, se pretende explorar cómo estas organizaciones perciben y gestionan estas amenazas y recopilar información detallada sobre sus prácticas actuales de ciberseguridad. Este análisis contribuirá a una comprensión integral del contexto empresarial en cuanto a la ciberseguridad, sirviendo como base para diseñar un plan de contingencia que incluya medidas preventivas, de detección, respuesta y recuperación.

De acuerdo con (Roberto Hernández Sampieri, 2014), la investigación descriptiva es fundamental para recolectar y organizar datos que permitan analizar fenómenos tal y como se presentan en un contexto específico. En este caso, la descripción del estado actual de las empresas en Honduras frente al ransomware proporcionará evidencia para fundamentar recomendaciones prácticas.

Justificación del Alcance Descriptivo

El ransomware es una amenaza global con impactos diferenciados dependiendo del nivel de preparación de las organizaciones. En el caso de Honduras, factores como la escasa inversión en tecnologías de ciberseguridad, el desconocimiento de mejores prácticas y la ausencia de normativas robustas incrementan significativamente la vulnerabilidad de las empresas.

Según Creswell (2018), un alcance descriptivo permite profundizar en las relaciones de causa y efecto dentro de un fenómeno complejo, como los ciberataques. Este alcance permite responder preguntas clave como:

- ¿Cuáles son las principales causas de los ciberataques exitosos?
- ¿Qué factores culturales, económicos o tecnológicos impiden la implementación de planes de contingencia eficaces?
- ¿Cómo afecta la falta de preparación a la continuidad operativa, la reputación y la sostenibilidad empresarial?

El análisis explicativo en esta investigación permitirá no solo identificar las deficiencias actuales, sino también justificar las estrategias recomendadas, como la capacitación en

ciberseguridad y la implementación de marcos internacionales adaptados al contexto local. Además, ayudará a justificar las recomendaciones específicas adaptadas al entorno empresarial hondureño, tales como:

- **Recomendaciones personalizadas para sectores clave:** Algunas industrias, como la banca y las telecomunicaciones, son más susceptibles debido al tipo de información tan importante que manejan.
- **Propuestas de capacitación:** La investigación explicará por qué es fundamental educar a los empleados en buenas prácticas de ciberseguridad, dado que la ingeniería social es un vector común en estos ataques.
- **Adaptación de marcos internacionales:** El análisis detallado de las causas permitirá proponer la implementación de estándares globales (como el NIST Cybersecurity Framework) ajustados a la realidad nacional.

Metodología Relacionada

Para alcanzar este nivel de profundidad, se utilizarán metodologías como:

Análisis de casos de estudio: Examinar incidentes de ransomware documentados en empresas hondureñas para identificar patrones comunes.

El enfoque explicativo no solo ayudará a desarrollar un plan integral, sino que también permitirá establecer las bases para futuras investigaciones en el ámbito de la ciberseguridad en Honduras. Al entender las causas del problema, se puede trabajar en estrategias preventivas y de mitigación que reduzcan la probabilidad y el impacto de futuros ataques, fortaleciendo la resiliencia digital de las empresas hondureñas.

3.3 DISEÑO

El estudio utilizará un diseño **descriptivo no experimental**. Este diseño permitirá analizar las variables relacionadas con los ataques de ransomware en empresas de Honduras, describiendo su impacto y explorando la relación entre variables clave como la frecuencia de ataques, los costos económicos, las medidas de seguridad implementadas y las políticas organizacionales. Las razones para adoptar este diseño son las siguientes:

- **Solidez Metodológica:** El diseño no experimental está respaldado por una base

metodológica robusta avalada por autores reconocidos, como Roberto Hernández Sampieri (2014).

- **Pertinencia al Contexto:** Este diseño es adecuado porque analiza el fenómeno del ransomware en su contexto natural, sin manipular las variables, lo que resulta ideal para estudiar cómo las empresas responden a este tipo de ciberataques.
- **Evidencia Empírica:** El diseño no experimental es eficaz para abordar problemas complejos como los relacionados con ciberseguridad y ransomware.
- **Consideraciones Éticas:** Al no implicar manipulación de variables ni intervención directa en las empresas participantes, este diseño respeta los principios éticos de la investigación científica.

3.3.1 POBLACIÓN

La población del estudio estará compuesta por empresas hondureñas, tanto pequeñas y medianas empresas (PyMEs) como grandes corporaciones, que operan en diversos sectores económicos y que han sido afectadas por incidentes de ransomware en los últimos años. Estas empresas incluyen tanto instituciones públicas como privadas, dado que el ransomware impacta de manera transversal en la economía. Se considerará a empresas con las siguientes características:

- Tamaño: pequeñas, medianas y grandes empresas.
- Sector: tecnológico, comercial, financiero, educativo y salud, entre otros.
- Ubicación: empresas ubicadas en diversas regiones de Honduras.

Dado que no es posible enumerar ni acceder a la totalidad de las empresas que cumplen con estas características, se considera que la población es **infinita**. Esto implica que no se trabajará con un marco muestral predefinido, sino con una selección estratégica que permita obtener datos significativos y variados.

3.3.2 MUESTRA

En este estudio se utilizará una muestra probabilística, ya que permite una selección representativa de la población y facilita el análisis de los resultados obtenidos. Debido a la naturaleza del estudio y la falta de un marco poblacional definido, se considerará que la población es infinita, por lo que el tamaño de la muestra se determinará utilizando la siguiente fórmula:

$$n = \frac{Z^2 * p * (1 - p)}{E^2}$$

Donde:

- n es el tamaño de la muestra
- Z es el valor para un nivel de confianza del 85% ($Z = 1.44$).
- p es la proporción esperada de la población con la característica de interés, en este caso un 0.5.
- E es el margen de error, en este caso de un 5%.

Remplazando los valores se obtiene el siguiente tamaño de la muestra:

$$n = \frac{1.44^2 * 0.5 * (1 - 0.5)}{0.05^2}$$

$$\boldsymbol{n = 207.36}$$

3.3.3 TÉCNICAS DE MUESTREO

Se empleará el muestreo **aleatorio simple**, el cual garantiza que cada elemento de la población tenga la misma probabilidad de ser seleccionado. Este método permite obtener datos representativos y evitar sesgos en la selección de los participantes.

Estas técnicas aseguran que los datos recopilados reflejen una diversidad adecuada y proporcionen información válida para el análisis del impacto y la respuesta ante los ataques de ransomware en el país.

3.4 CRITERIOS DE SELECCIÓN DE LA MUESTRA

Dado que la investigación se centra en empresas de Honduras, es crucial definir criterios claros para seleccionar a los participantes que formarán parte del estudio. Esto garantizará que los datos obtenidos sean representativos y relevantes.

3.4.1 CRITERIOS DE INCLUSIÓN

Los criterios de inclusión se fundamentan en la necesidad de focalizar la investigación en empresas con características que permitan identificar patrones de vulnerabilidades comunes frente

al ransomware. Esto incluye organizaciones de sectores críticos (banca, salud, telecomunicaciones), las cuales manejan grandes volúmenes de información sensible. Siguiendo la opinión de Peltier (2010), las empresas con alta dependencia tecnológica están particularmente expuestas a ataques cibernéticos debido a la integración de tecnologías emergentes y la falta de políticas de seguridad robustas. Este enfoque garantiza la relevancia de los datos recopilados para desarrollar planes de contingencia eficaces. Para garantizar que los datos obtenidos sean pertinentes y útiles para los objetivos de la investigación, se consideran los siguientes criterios de inclusión:

Empresas de sectores críticos:

Se priorizarán empresas de sectores clave como banca, telecomunicaciones, salud y logística, ya que manejan grandes volúmenes de datos sensibles y son más propensas a ser atacadas.

Empresas con historial de ciber incidentes:

Se incluirán aquellas empresas que hayan reportado al menos un intento de ciberataque en los últimos tres años, ya que estas ofrecen un panorama claro sobre las vulnerabilidades actuales y la efectividad de las medidas implementadas.

Ubicación geográfica en Honduras:

Solo se considerarán empresas ubicadas en territorio hondureño, para garantizar que los resultados sean aplicables al contexto nacional.

Disponibilidad para participar:

Las empresas deberán mostrar disposición para colaborar proporcionando información sobre sus políticas de ciberseguridad, medidas actuales y experiencia con ransomware.

3.4.2 CRITERIOS DE EXCLUSIÓN

Para mantener un enfoque claro y evitar datos irrelevantes, se han definido los siguientes criterios de exclusión:

Microempresas:

Las empresas con menos de 50 empleados serán excluidas debido a la limitada complejidad de sus sistemas informáticos y recursos tecnológicos.

Falta de acceso a información relevante:

Empresas que no estén dispuestas a proporcionar información detallada sobre su infraestructura de ciberseguridad o su experiencia con ciberataques serán excluidas del estudio.

Empresas sin un enfoque digital:

Las organizaciones que no dependan de sistemas informáticos o que tengan una mínima exposición digital serán descartadas, ya que no representan objetivos típicos de ransomware.

Sectores no críticos:

Se excluirán empresas de sectores no estratégicos o que no manejen datos sensibles, como negocios de comercio minorista o empresas familiares pequeñas.

Justificación de los Criterios

Los criterios definidos aseguran que la investigación se centre en empresas de sectores estratégicos, caracterizadas por su elevada exposición a riesgos de ciberataques debido a su dependencia tecnológica y al manejo de información crítica. Para Skouby et al, (2017), las organizaciones que operan en infraestructuras críticas como salud, energía y finanzas presentan una mayor vulnerabilidad frente al ransomware debido a la combinación de su complejidad operativa y la importancia de su información para la continuidad del negocio. Este enfoque no solo permitirá diseñar un plan de contingencia adaptable, sino también garantizar que las estrategias sean efectivas y aplicables a los entornos más amenazados.

3.5 HIPÓTESIS (No aplica)

De acuerdo con Creswell et al, (2018), a investigación cualitativa se centra en la comprensión y descripción de experiencias, percepciones o fenómenos desde la perspectiva de los participantes, sin ideas preconcebidas que deban ser probadas. Por lo tanto, la formulación de hipótesis no es un requisito en este tipo de estudios, ya que su objetivo no es verificar predicciones o relaciones específicas entre variables, a diferencia de la investigación cuantitativa.

Creswell et al, (2018), enfatizan que, en una investigación cualitativa descriptiva, el investigador se concentra en describir un fenómeno o situación tal como ocurre en su contexto natural, sin intentar explicar sus causas o hacer predicciones sobre él. Por esta razón, las investigaciones de este tipo suelen formular preguntas de investigación amplias y abiertas, en lugar

de hipótesis específicas que se deben probar.

3.6 OPERACIONALIZACIÓN DE LAS VARIABLES

Tabla 8 Operacionalización de las variables

Variable	Tipo	Definición Conceptual	Definición Operacional	Indicador	Dimensión	Escala de medición
Experiencia con ransomware	Independiente	Percepción y vivencia de las personas afectadas por ransomware en Honduras	Entrevistas en profundidad con víctimas de ransomware, análisis de casos de estudio	Narrativas de las experiencias, estrategias de respuesta, impacto emocional y económico	Impacto personal y social	Nominal (presente/ausente), ordinal (nivel de impacto)
Conocimiento sobre ransomware	Independiente	Nivel de conocimiento de las personas sobre qué es el ransomware, cómo funciona y cómo prevenirlo.	Cuestionarios abiertos, grupos focales con diferentes actores (empresas, gobierno, ciudadanos)	Conceptos clave mencionados, nivel de detalle en las respuestas, identificación de fuentes de información	Conocimiento y percepción del riesgo	Nominal (alto/medio/bajo), ordinal (nivel de conocimiento)
Respuestas organizacionales	Independiente	Acciones y estrategias implementadas por organizaciones públicas y privadas para prevenir y responder a ataques de ransomware en Honduras	Análisis de documentos (políticas, protocolos), entrevistas con responsables de seguridad informática	Estrategias de prevención, planes de respuesta a incidentes, inversión en seguridad cibernética	Preparación y respuesta	Nominal (existencia/ausencia), ordinal (nivel de preparación)

Fuente: Elaboración propia

3.7 TÉCNICAS, INSTRUMENTOS Y PROCEDIMIENTOS APLICADOS

3.7.1 TÉCNICAS

En esta investigación cualitativa, se emplearán técnicas que integran tanto la recopilación de información primaria como el análisis de fuentes secundarias. Estas técnicas permitirán una comprensión profunda y contextual del impacto del ransomware en empresas hondureñas.

Análisis documental (fuentes secundarias)

Se realizará una revisión exhaustiva de reportes de ciberseguridad, estudios de casos, normativas internacionales, informes técnicos y estadísticas publicadas por organizaciones como empresas de ciberseguridad, organismos internacionales y gobiernos de otros países. Este análisis permitirá complementar los datos primarios con información contextual y patrones globales.

Entrevistas semiestructuradas

Según Roberto Hernández Sampieri (2014), las entrevistas semiestructuradas se basan en una guía de asuntos o preguntas y el entrevistador tiene la libertad de introducir preguntas adicionales para precisar conceptos u obtener más información. Se llevarán a cabo entrevistas con actores clave como gerentes de TI, administradores de seguridad y otros profesionales relacionados con la gestión de ciberseguridad en empresas hondureñas. Este enfoque permitirá obtener narrativas sobre experiencias y estrategias de respuesta ante ransomware.

3.7.2 INSTRUMENTOS

Los instrumentos de recolección de datos están diseñados para capturar información tanto de fuentes primarias como secundarias:

Plantilla de análisis documental

Herramienta clave para sistematizar la información proveniente de fuentes secundarias, como reportes de ransomware, estadísticas globales, guías de ciberseguridad, y estudios realizados por empresas tecnológicas internacionales. Este instrumento incluirá campos para registrar datos como el origen del documento, variables analizadas (frecuencia de ataques, costos económicos, etc.) y hallazgos relevantes.

Guía de entrevistas semiestructuradas

Documento que incluirá preguntas abiertas y cerradas adaptadas para obtener detalles específicos sobre la percepción de las empresas hondureñas ante el ransomware. El formato de la encuesta será el siguiente y será aplicado mediante Microsoft Forms.

3.7.3 PROCEDIMIENTOS

Los procedimientos estarán orientados a combinar datos primarios y secundarios de forma sistemática, asegurando un análisis integral del fenómeno estudiado:

Revisión inicial de fuentes secundarias:

- Realizar una búsqueda de reportes, estadísticas y estudios de casos internacionales y nacionales relacionados con ransomware.
- Identificar patrones relevantes en las tendencias globales para contextualizar los hallazgos locales.

Selección de participantes y recopilación de datos primarios:

- Contactar a empresas hondureñas afectadas por ransomware y coordinar entrevistas con gerentes o responsables de TI.
- Registrar las experiencias de los participantes sobre cómo afrontaron y gestionaron los incidentes.

Integración de datos secundarios:

- Complementar las narrativas obtenidas en las entrevistas con los hallazgos documentales.
- Comparar estadísticas globales con las percepciones y casos específicos de Honduras para identificar similitudes y diferencias clave.

Consolidar Información:

- Consolidar la información obtenida de entrevistas, observaciones y análisis documental para construir un panorama detallado y balanceado del impacto del ransomware en las empresas hondureñas.

3.7.4 PLAN DE ANÁLISIS

El plan de análisis se diseñará para integrar los datos provenientes de fuentes secundarias y primarias, favoreciendo una comprensión amplia y contextualizada:

Tabla 9 Plan de análisis de la investigación

Fase	Descripción	Herramientas	Objetivo
Recopilación de datos	- Revisión de informes técnicos y reportes globales sobre ransomware publicados entre 2020 y 2024. - Búsqueda de normativas, estudios y estadísticas de ciberseguridad.	Repositorios en línea de empresas de ciberseguridad, como Kaspersky y Symantec. Bases de datos	- Identificar patrones internacionales y nacionales del impacto del ransomware. - Complementar la información obtenida en

Fase	Descripción	Herramientas	Objetivo
		académicas (Google Scholar, Scopus).	entrevistas.
Organización y clasificación	- Clasificación de los datos en categorías temáticas: costos, métodos de ataque, sectores afectados. - Sistematización de información relevante proveniente de fuentes primarias y secundarias.	- Software de análisis cualitativo (NVivo, Atlas.ti). - Hojas de cálculo (Excel, Google Sheets).	- Garantizar que los datos estén estructurados para facilitar su análisis. - Preparar las bases para la triangulación de información.
Codificación y análisis temático	- Identificación de patrones y relaciones entre las variables estudiadas. - Análisis de similitudes y diferencias entre hallazgos de entrevistas y reportes documentales.	- Software de análisis cualitativo (NVivo, Atlas.ti).	-Explorar las conexiones entre las experiencias locales y los contextos globales. - Desarrollar categorías temáticas relevantes.
Interpretación y síntesis	- Relación de los hallazgos con los objetivos de la investigación. - Elaboración de conclusiones basadas en la integración de datos primarios y secundarios.	- Procesadores de texto (Word). - Gráficos y mapas conceptuales (Miro, Lucidchart).	- Extraer implicaciones prácticas y teóricas. - Proponer estrategias adaptadas a la realidad de las empresas hondureñas.

Fuente: Elaboración propia

3.8 FUENTES DE INFORMACIÓN

Las fuentes de información son los recursos o materiales que proporcionan datos relevantes, útiles y verificables para la construcción y desarrollo de un estudio o investigación. Estas fuentes se clasifican comúnmente en **primarias**, **secundarias** y, en algunos casos, **terciarias**, dependiendo del nivel de originalidad y tratamiento de los datos que contienen.

3.8.1 FUENTES PRIMARIAS

Las fuentes primarias se obtendrán directamente de las empresas hondureñas seleccionadas para el estudio. Estas incluirán:

- **Encuesta estructurada:** Se aplicarán cuestionarios a profesionales de ciberseguridad y TI en empresas hondureñas para evaluar el nivel de preparación ante ataques de ransomware. Estas encuestas incluirán preguntas sobre el uso de herramientas de seguridad, frecuencia de actualizaciones y existencia de planes de contingencia. Ver **anexo 1**.
- **Entrevista a profundidad:** Se realizarán entrevistas con expertos en seguridad informática y respuesta a incidentes, quienes compartirán su experiencia sobre ataques previos en Honduras, estrategias utilizadas para mitigarlos y desafíos que enfrentan las

organizaciones en la implementación de medidas de protección. Ver **anexo 2.**

- **Estudios de caso**s: Se analizarán empresas hondureñas que han sido víctimas de ransomware, examinando la respuesta que implementaron, el impacto operativo y financiero sufrido, y qué acciones tomaron para mejorar su seguridad después del ataque.

3.8.2 FUENTES SECUNDARIAS

Las fuentes secundarias serán fundamentales para contextualizar el estudio y fundamentar teóricamente las estrategias propuestas. Estas incluirán:

- **Normativas y estándares internacionales:** La investigación utilizará la ISO 22301 y la ISO 27001 como referencia para diseñar un plan de contingencia adaptado al contexto hondureño, garantizando el cumplimiento de mejores prácticas en continuidad del negocio y protección de la información.
- **Informes técnicos y reportes de ciberseguridad:** Se emplearán estudios de empresas especializadas como SOPHOS, Check Point y Kaspersky, que brindan datos recientes sobre el crecimiento de los ataques de ransomware en América Latina y las herramientas más efectivas para combatirlos.
- **Documentación gubernamental y reportes de organismos internacionales**: Se consultarán documentos de la OEA, el Banco Interamericano de Desarrollo (BID) y CONATEL, que analizan el estado actual de la ciberseguridad en Honduras y ofrecen recomendaciones para mejorar la protección de infraestructuras críticas.

3.9 MATRIZ DE CONGRUENCIA

Tabla 10 Matriz de congruencia

Nombre de la investigación	Problema	Pregunta(s) de Investigación	Objetivos de la Investigación	Metodología	Instrumentos	Variables	Indicadores
Fortalecimiento de la ciberseguridad en empresas hondureñas mediante un plan de contingencia para ataques de ransomware.	Las empresas hondureñas presentan una creciente vulnerabilidad frente a los ataques de ransomware, lo cual compromete la seguridad de su información, la continuidad de sus operaciones y su reputación en el mercado. Las deficiencias en medidas preventivas, así como la falta de un plan integral de contingencia, agravan esta situación.	**General:** ¿Cuáles son las principales vulnerabilidades y factores de riesgo de las empresas hondureñas frente a ataques de ransomware, y cómo puede diseñarse un plan de contingencia efectivo para abordar estas amenazas?	**General:** Diseñar un plan de contingencia para la prevención, detección, respuesta y recuperación frente a ataques de tipo ransomware en empresas hondureñas.	Investigación cualitativa con alcance descriptivo. Se empleará análisis de contenido, entrevistas a profundidad y revisión de casos documentados.	Guías de entrevistas, fichas de análisis documental, matrices de categorización de datos.	**Independiente:** Nivel de preparación ante ciberataques (categórica).	- Número de empresas con un plan de contingencia documentado. - Tipos de medidas preventivas implementadas. - Incidencia de ransomware en el sector privado en el último año.
		Específicas: - ¿Qué factores técnicos, organizacionales y humanos contribuyen a la exposición de las empresas a ataques de ransomware? - ¿Cuáles son las prácticas actuales de ciberseguridad y cómo impactan en la prevención y respuesta a estos ataques?	**Específicos**: - Identificar las principales vulnerabilidades y factores de riesgo en empresas hondureñas. - Analizar las prácticas actuales de ciberseguridad utilizadas por las empresas en Honduras. - Proponer estrategias concretas basadas en normas internacionales (ISO 22301 e ISO 27001).			**Dependientes:** - Vulnerabilidades técnicas (categórica). - Factores humanos y organizativos (categórica). - Existencia de un plan de contingencia (dicotómica).	

Fuente: Elaboración propia

CAPÍTULO IV – RESULTADOS Y ANALISIS

La seguridad de la información en las empresas hondureñas enfrenta desafíos significativos debido al incremento de los ataques de ransomware y la escasa preparación para gestionarlos de manera efectiva. A través del proceso de recopilación de información, se ha evidenciado que muchas organizaciones carecen de controles adecuados y no cuentan con planes de contingencia estructurados, lo que incrementa su vulnerabilidad ante este tipo de amenazas.

En este capítulo se presentan los hallazgos obtenidos a partir del análisis de los datos recopilados mediante encuestas, entrevistas con especialistas en ciberseguridad, estudios de casos y revisión de documentación relevante. Se identifican las principales vulnerabilidades y factores de riesgo que afectan a las empresas, así como las estrategias actuales de prevención, detección y respuesta ante ataques de ransomware. Asimismo, se evalúa el nivel de implementación y efectividad de los planes de contingencia en Honduras, resaltando las deficiencias que podrían comprometer la continuidad operativa y la seguridad de la información.

Los resultados de este análisis servirán como base para el diseño de un plan de contingencia y respuesta adaptado al contexto hondureño, alineado con normativas internacionales y mejores prácticas de seguridad. Esto permitirá fortalecer la resiliencia de las empresas frente a los ciberataques, minimizando el impacto operativo y financiero que pueden generar.

4.1 ANÁLISIS EXPLORATORIO DE DATOS

4.1.1 DESCRIPCIÓN GENERAL DEL CONJUNTO DE DATOS

El conjunto de datos analizado en este estudio está compuesto por un total de 207 encuestados. La muestra fue seleccionada utilizando un método de muestreo aleatorio simple, asegurando una representación adecuada de la población objetivo. Los encuestados incluyen profesionales con distintos roles dentro de las empresas, como gerentes de TI, oficiales de ciber seguridad, desarrolladores de software, ingenieros de infraestructura y personal de soporte técnico, lo que permite obtener una visión integral sobre la ciberseguridad en el sector. Además, la muestra incluye empresas de diversas regiones del país, lo que permite analizar y comparar los diferentes niveles de madurez en ciberseguridad frente a ataques de ransomware. Esta diversidad geográfica brinda una perspectiva más amplia sobre las capacidades y desafíos que enfrentan las empresas en la prevención, detección y respuesta ante este tipo de amenazas. Ver **anexo 3**.

Tabla 11 Variables Bajo Estudio

Fase	Descripción
Experiencia con ransomware	Frecuencia con la que las empresas han sido víctimas de ataques de ransomware, ya sea una o varias veces.
Sector empresarial	Tipo de industria en la que opera la empresa (Finanzas, Gobierno, Educación, TI, etc.).
Tamaño de la empresa	Cantidad aproximada de empleados en la empresa, clasificada en rangos (1-20, 20-50, 50-100, más de 100).
Departamento de ciberseguridad	Existencia y modalidad de un equipo de seguridad informática en la empresa (interno, tercerizado, gestionado por TI o inexistente).
Medidas preventivas	Estrategias implementadas para prevenir ataques de ransomware, como copias de seguridad, firewalls, autenticación multifactor, entre otras.
Frecuencia de actualización de políticas	Periodicidad con la que se revisan y actualizan las políticas de ciberseguridad en la empresa.
Percepción sobre la concienciación en Honduras	Opinión de los encuestados sobre el nivel de conocimiento en ciberseguridad en el sector empresarial del país.
Barreras para mejorar la ciberseguridad	Factores que dificultan la implementación de mejores medidas de seguridad en las empresas (falta de presupuesto, personal, concienciación, etc.).
Uso de copias de seguridad	Regularidad con la que las empresas realizan respaldos de su información (diario, semanal, mensual, nunca).
Plan de contingencia	Existencia de un plan documentado para responder a ataques de ransomware y si ha sido probado mediante simulacros.
Acciones prioritarias ante un ataque	Estrategias que la empresa considera más importantes en caso de un ataque de ransomware.

Fuente: Elaboración propia

4.1.2 LIMPIEZA Y PREPARACIÓN DE DATOS

Para garantizar que el análisis de los datos recopilados sobre ciberseguridad y ransomware en empresas de Honduras sea preciso y confiable, se llevó a cabo un proceso estructurado de limpieza y preparación de datos utilizando Python. A continuación, se describen los pasos realizados:

1. **Importación de Datos:** Los datos fueron importados desde archivos CSV utilizando la biblioteca Pandas, una herramienta ampliamente utilizada en el análisis de datos en Python. Este proceso permitió cargar la información de manera estructurada en un DataFrame, lo que facilitó su manipulación y exploración posterior. Ver **anexo 4.**

0	1	2/8/2025 13:17	2/8/2025 13:21	anonymous	NaN	Manufactura	Más de 100 empleados	No, la seguridad es gestionada por el equipo d...	Sí, en más de una ocasión	NaN	Copias de seguridad regulares;Firewalls y sist...	Cada año	
1	2	2/9/2025 13:01	2/9/2025 13:07	anonymous	NaN	Comunicaciones	Más de 100 empleados	Sí, pero tercerizamos el servicio	Sí, una sola vez	Primero revisar los daños, seguido de ello res...	Copias de seguridad regulares;Firewalls y sist...	Cada 6 meses o menos	a
2	3	2/9/2025 13:03	2/9/2025 13:07	anonymous	NaN	Educación	Más de 100 empleados	No, la seguridad es gestionada por el equipo d...	Sí, una sola vez	Acción rápida por parte del equipo y rastreo y...	Copias de seguridad regulares;Firewalls y sist...	Cada año	
3	4	2/9/2025 13:08	2/9/2025 13:12	anonymous	NaN	Logística	Entre 50 - 100 empleados	Sí, con personal especializado interno	No, pero hemos detectado intentos	NaN	Copias de seguridad regulares;Firewalls y sist...	Cada año	
4	5	2/9/2025 13:39	2/9/2025 13:46	anonymous	NaN	Gobierno	Más de 100 empleados	No, la seguridad es gestionada por el equipo d...	No, pero hemos detectado intentos	NaN	Copias de seguridad regulares;Firewalls y sist...	No contamos con políticas documentadas	

Figura 8 Importación de Pandas
Fuente: Elaboración Propia.

2. **Cambio en nombres de Columnas:** Tras la importación del archivo CSV, se realizó un ajuste en los nombres de las columnas, ya que los originales eran demasiado extensos. Esta simplificación facilita la manipulación de los datos, mejora la legibilidad y optimiza el análisis posterior, evitando confusiones o dificultades al referirse a cada variable dentro del conjunto de datos.

	Id	¿En qué sector opera su empresa? (Si su sector no está en la lista, no dude en especificarlo)	¿Cuál es el número aproximado de empleados en su empresa?	¿Cuenta su empresa con un departamento o equipo de ciberseguridad?	¿Su empresa ha sido víctima de algún ataque de ransomware recientemente?	¿podría compartir brevemente cómo manejaron la situación?	¿Qué medidas preventivas utiliza su empresa contra el ransomware? (Marque todas las que correspondan)\n	¿Cada cuánto se actualizan las políticas de ciberseguridad en su empresa?	En caso de un ataque de ransomware, ¿qué acción tomaría su empresa como prioridad? (Clasifique del 1 al 5)	¿Utilizan sistemas de respaldo de información regularmente?	¿Cuenta su empresa con un plan de contingencia documentado en caso de ataque de ransomware?
0	1	Manufactura	Más de 100 empleados	No, la seguridad es gestionada por el equipo d...	Sí, en más de una ocasión	NaN	Copias de seguridad regulares;Firewalls y sist...	Cada año	Aislar sistemas y contactar a especialistas en...	Sí, diario	Sí, pero no ha sido probadc
1	2	Comunicaciones	Más de 100 empleados	Sí, pero tercerizamos el servicio	Sí, una sola vez	Primero revisar los daños, seguido de ello res...	Copias de seguridad regulares;Firewalls y sist...	Cada 6 meses o menos	Reportarlo a las autoridades;Aislar sistemas y...	Sí, semanal	Sí, pero no ha sido probadc
2	3	Educación	Más de 100 empleados	No, la seguridad es gestionada por el equipo d...	Sí, una sola vez	Acción rápida por parte del equipo y rastreo y...	Copias de seguridad regulares;Firewalls y sist...	Cada año	Aislar sistemas y contactar a especialistas en...	Sí, mensual	No, perc estamos desarrollándolc
3	4	Logística	Entre 50 - 100 empleados	Sí, con personal especializado interno	No, pero hemos detectado intentos	NaN	Copias de seguridad regulares;Firewalls y sist...	Cada año	Aislar sistemas y contactar a especialistas en...	Sí, diario	No tenemos ur plar documentadc
4	5	Gobierno	Más de 100 empleados	No, la seguridad es gestionada por el equipo d...	No, pero hemos detectado intentos	NaN	Copias de seguridad regulares;Firewalls y sist...	No contamos con políticas documentadas	No tenemos un plan de acción definido;Aislar s...	Sí, diario	No tenemos ur plar documentadc

Figura 9 Columnas con Nombres Originales
Fuente: Elaboración Propia.

	Id	Empresa	NumeroEmpleados	EquipoSeguridad	Victima	ManejoSituacion	Medidas	Politicas	PrioridadRansomware	Respaldos	PlanCon
0	1	Manufactura	Más de 100 empleados	No, la seguridad es gestionada por el equipo d...	Sí, en más de una ocasión	NaN	Copias de seguridad regulares;Firewalls y sist...	Cada año	Aislar sistemas y contactar a especialistas en...	Sí, diario	Sí, pero
1	2	Comunicaciones	Más de 100 empleados	Sí, pero tercerizamos el servicio	Sí, una sola vez	Primero revisar los daños, seguido de ello res...	Copias de seguridad regulares;Firewalls y sist...	Cada 6 meses o menos	Reportarlo a las autoridades;Aislar sistemas y...	Sí, semanal	Sí, pero
2	3	Educación	Más de 100 empleados	No, la seguridad es gestionada por el equipo d...	Sí, una sola vez	Acción rápida por parte del equipo y rastreo y...	Copias de seguridad regulares;Firewalls y sist...	Cada año	Aislar sistemas y contactar a especialistas en...	Sí, mensual	No, per desar
3	4	Logística	Entre 50 - 100 empleados	Sí, con personal especializado interno	No, pero hemos detectado intentos	NaN	Copias de seguridad regulares;Firewalls y sist...	Cada año	Aislar sistemas y contactar a especialistas en...	Sí, diario	No te doc
4	5	Gobierno	Más de 100 empleados	No, la seguridad es gestionada por el equipo d...	No, pero hemos detectado intentos	NaN	Copias de seguridad regulares;Firewalls y sist...	No contamos con políticas documentadas	No tenemos un plan de acción definido;Aislar s...	Sí, diario	No te doc
...	...	...	...	...	...	...	...	...	...	...	

Figura 10 Columnas con Nombres Modificados
Fuente: Elaboración Propia.

3. **Análisis de Datos Faltantes**: Para evaluar la calidad de los datos y detectar posibles inconsistencias, se realizó un análisis exhaustivo de los valores faltantes. Primero, se llevó a cabo un conteo de valores nulos por columna para identificar qué variables presentaban información incompleta y en qué magnitud. Posteriormente, se generó un mapa de valores faltantes, lo que permitió visualizar la distribución de los datos ausentes y analizar posibles patrones de omisión. Este análisis fue fundamental para decidir las estrategias de manejo de datos faltantes, asegurando la integridad y fiabilidad del conjunto de datos antes de su procesamiento. Ver **anexo 5.**

```
Valores faltantes por columna:
Id                      0
Empresa                 0
NumeroEmpleados         1
EquipoSeguridad         0
Victima                 0
ManejoSituacion        10
Medidas\r\n             0
Politicas               0
PrioridadRansomware     0
Respaldos               0
PlanContingencia        0
Barreras\r\n            0
Conciencia              0
Estrategias\r\n         0
Comentarios\r\n        13
```

Figura 11 Valores Faltantes por Columna
Fuente: Elaboración Propia.

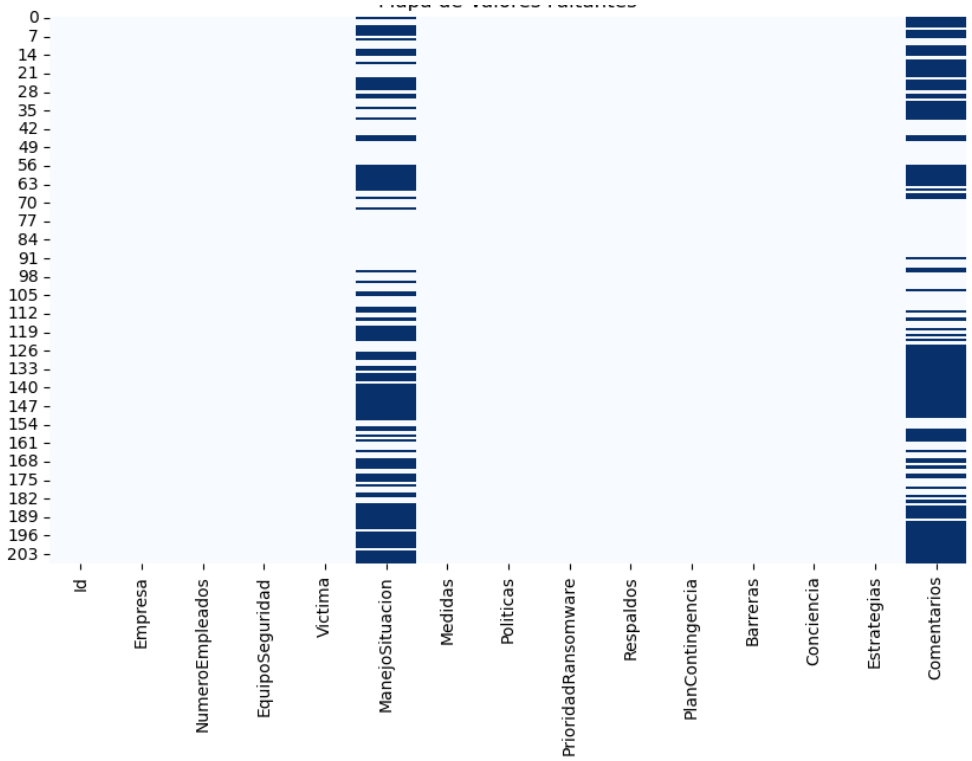


Figura 12 Mapa de Valores Faltantes
Fuente: Elaboración Propia.

4. **Limpieza y Transformación de Datos:** Una vez identificadas las columnas con valores faltantes, se procedió a su tratamiento para garantizar la integridad del conjunto de datos. En el caso de las respuestas sin información, se reemplazaron los valores nulos con la etiqueta "No especificado", asegurando que no se perdiera información relevante y manteniendo la coherencia en el análisis. Además, para evaluar la correlación entre variables, las variables categóricas fueron transformadas a formato numérico mediante un proceso de codificación, permitiendo su uso en análisis estadísticos y modelado de datos. Estas transformaciones facilitaron la interpretación de los resultados y la aplicación de técnicas de análisis más avanzadas.

5. **Visualización Mediante Matplotlib y Seaborn**: Una vez que el conjunto de datos fue limpiado y preparado, se emplearon las bibliotecas Matplotlib y Seaborn para su representación gráfica. Estas herramientas permitieron visualizar la distribución de las variables, identificar patrones y tendencias, y facilitar la interpretación de los datos.

4.1.3 VISUALIZACIÓN DE DATOS

Pregunta 1.

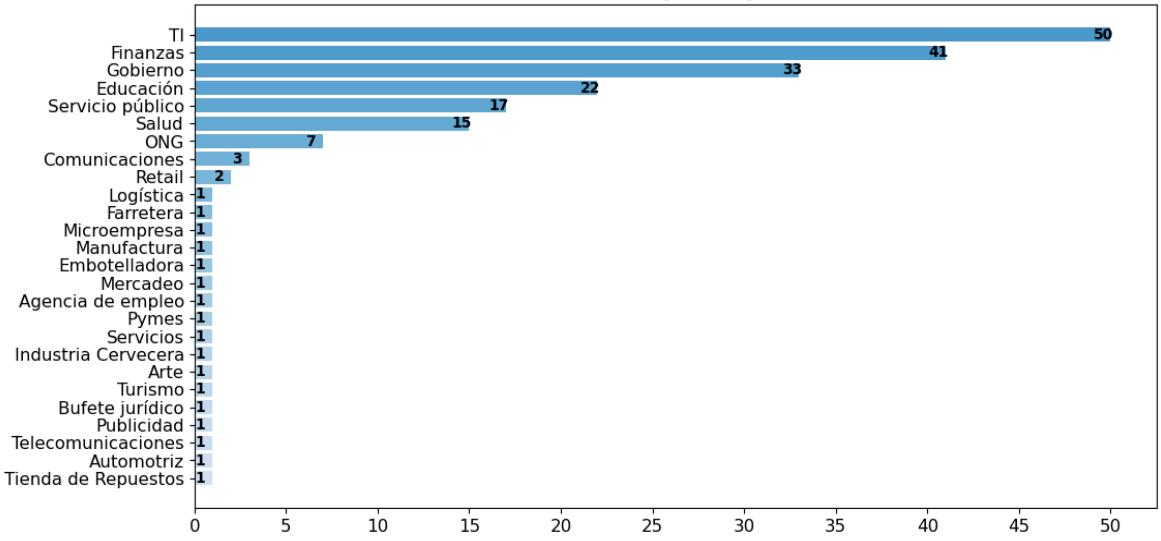


Figura 13 Cantidad de Empresas por Sector
Fuente: Elaboración Propia.

El gráfico muestra la distribución de las empresas encuestadas según su sector de operación. Se observa que el sector de Tecnologías de la Información (TI) es el más representado, con **50 empresas**, seguido por el sector gubernamental (**33 empresas**), el sector financiero (**41 empresas**) y el de educación (**22 empresas**). Otros sectores con una representación significativa incluyen el servicio público (**17 empresas**) y salud (**15 empresas**), mientras que el resto de los sectores tienen una presencia menor, con una o pocas empresas cada uno.

Estos datos reflejan una fuerte participación de sectores estratégicos en la encuesta, donde los sectores con mayor dependencia de la tecnología y la infraestructura digital, como TI, finanzas y gobierno, tienen una mayor presencia. La diversidad de sectores representados en la muestra permite un análisis más completo de la situación de la ciberseguridad en distintas áreas económicas del país, evidenciando la necesidad de fortalecer las estrategias de protección y contingencia ante ataques como el ransomware.

La distribución casi equitativa en otros sectores también sugiere que el impacto del ransomware no es exclusivo de un solo rubro, sino que afecta a distintos tipos de organizaciones, independientemente de su actividad económica. Esto refuerza la necesidad de estrategias de seguridad adaptadas a las particularidades de cada industria.

Pregunta 2

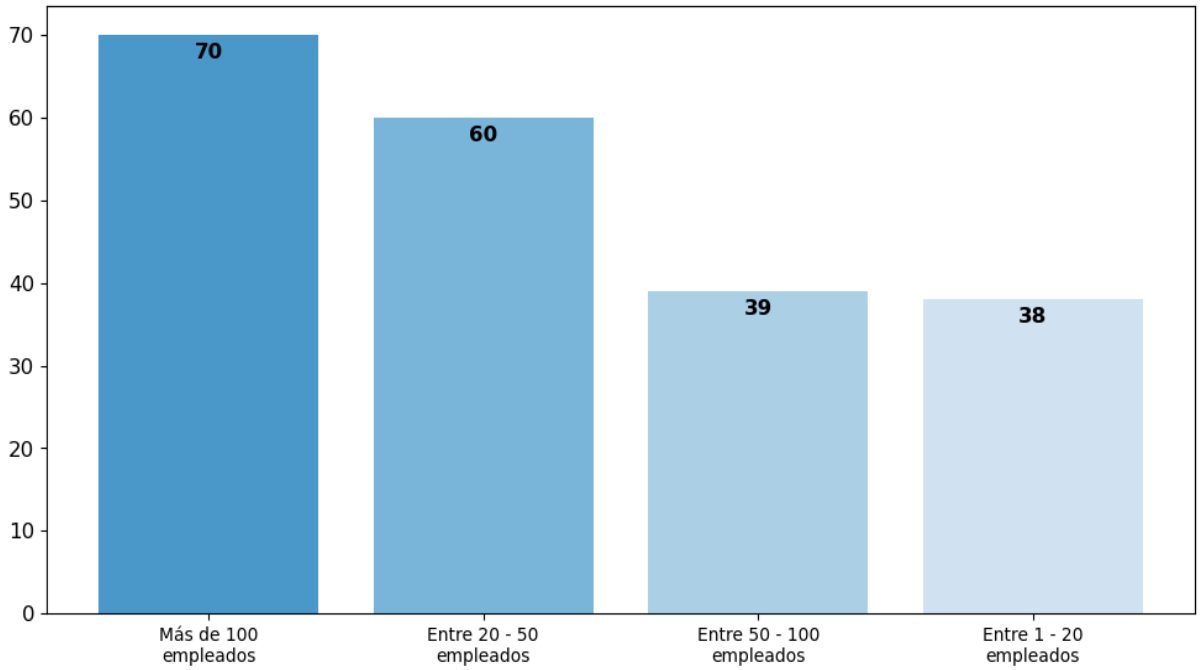


Figura 14 Cantidad de Empleados por Numero
Fuente: Elaboración Propia.

El gráfico muestra la distribución de las empresas encuestadas según su cantidad de empleados. Se observa que la mayoría de las (**70 empresas**) tienen "**más de 100 empleados",** lo que indica una alta participación de organizaciones de gran tamaño en la encuesta.

En segundo lugar, se encuentran las empresas con "entre 20 y 50 empleados" (**60 empresas**), seguidas por aquellas con "entre 1 y 20 empleados" (**38 empresas**). Finalmente, (**39 empresas)** reportaron tener "entre 50 y 100 empleados", de esta forma todos y cada uno de los encuestados especificó el rango de la cantidad de empleados en las que sus empresas andan.

Estos resultados reflejan que las empresas participantes varían en tamaño, lo que permite analizar cómo las estrategias de ciberseguridad y los planes de contingencia pueden diferir según la cantidad de empleados. Es posible que las empresas más pequeñas tengan menos recursos dedicados a la seguridad informática, lo que podría aumentar su vulnerabilidad ante amenazas como el ransomware.

Pregunta 3

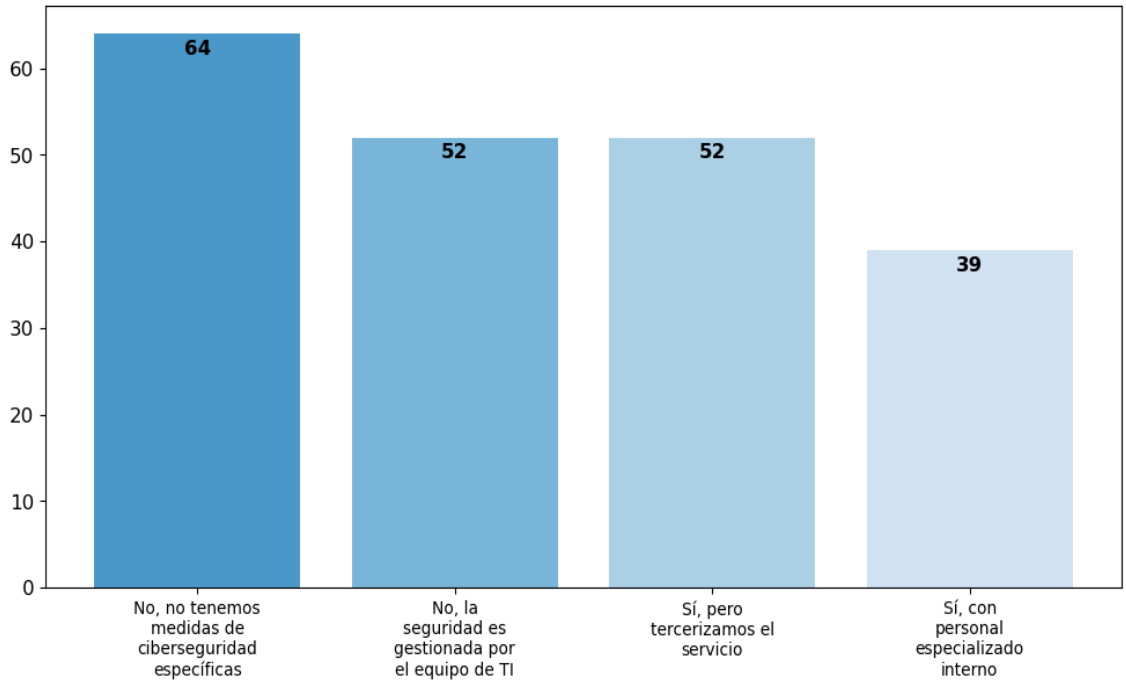


Figura 15 Disponibilidad de Equipo de Ciberseguridad
Fuente: Elaboración Propia.

En el gráfico se refleja la disponibilidad de un equipo de ciberseguridad en las empresas encuestadas. Se observa que (**64 empresas)** indicaron que "**no cuentan con medidas de ciberseguridad específicas"**, lo que evidencia una preocupante falta de controles dedicados a la protección contra amenazas cibernéticas en el país.

Por otro lado, (**52 empresas)** señalaron que "la seguridad es gestionada por el **equipo de TI"**, lo que sugiere que, si bien hay cierto nivel de protección, no existe un equipo especializado en ciberseguridad. Además, (**52 empresas)** afirmaron que **"tercerizan el servicio"**, lo que puede implicar dependencia de proveedores externos y posibles limitaciones en tiempos de respuesta ante incidentes.

Finalmente, solo (**39 empresas)** cuentan con "**personal especializado interno"** en ciberseguridad, lo que indica que una minoría de las organizaciones posee una estructura dedicada exclusivamente a la protección de su infraestructura tecnológica. Estos resultados destacan la necesidad de fomentar la creación de equipos especializados y la adopción de estrategias más robustas en ciberseguridad, especialmente ante amenazas como el ransomware.

Pregunta 4

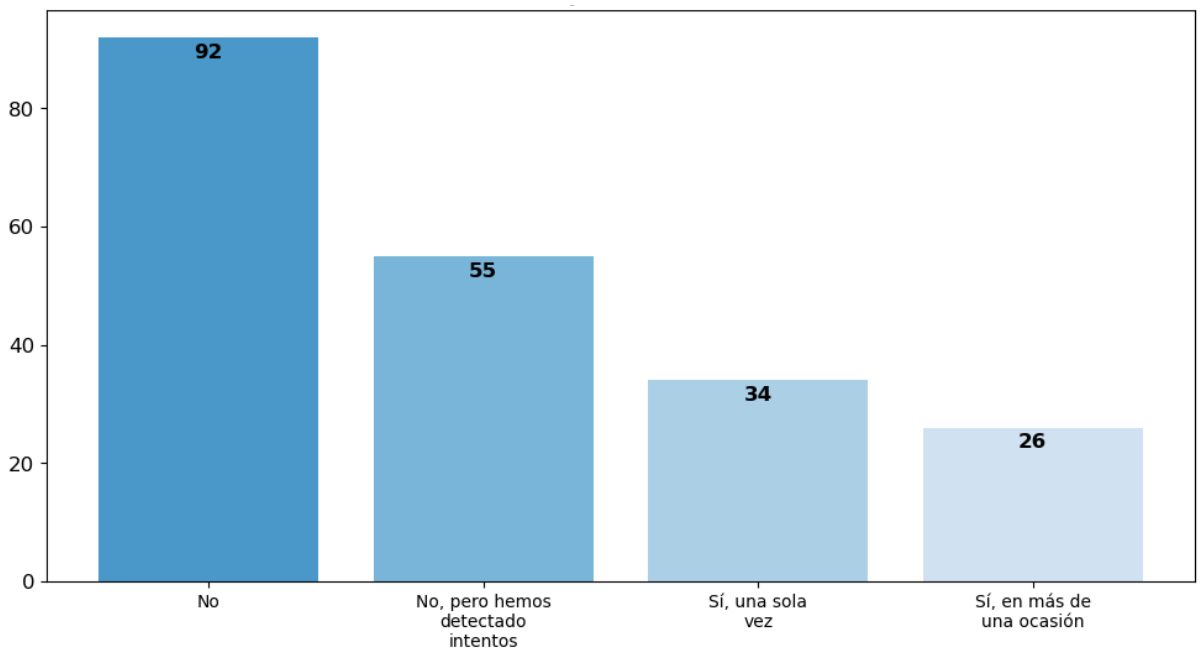


Figura 16 Victimas por Ransomware
Fuente: Elaboración Propia.

Los resultados obtenidos en esta pregunta muestran que (**92 empresas),** indicaron que **"no han sido víctimas de ataques de ransomware"**, lo cual es positivo, aunque no necesariamente indica que estén exentas de riesgos solo por no haber sido víctimas. Sin embargo, (**55 empresas**) afirmaron haber **"detectado intentos de ataque**", lo que sugiere que la amenaza del ransomware es una preocupación latente en el entorno empresarial hondureño.

Por otro lado, y el dato más preocupante es que, (**34 empresas**) han sido "**víctimas de ransomware al menos una vez**", mientras que (**26 empresa**s) han sufrido "**múltiples ataques**", lo que refleja una vulnerabilidad considerable en ciertas organizaciones. Estos datos ponen en evidencia la importancia de fortalecer las estrategias de prevención y respuesta ante incidentes, ya que un número significativo de empresas ha experimentado ataques directos o intentos de intrusión.

Ante esta realidad, se vuelve crucial la implementación de planes de contingencia, medidas de ciberseguridad más robustas y capacitación continua del personal, con el objetivo de reducir la exposición al ransomware y mitigar su impacto en las operaciones empresariales.

Pregunta 5

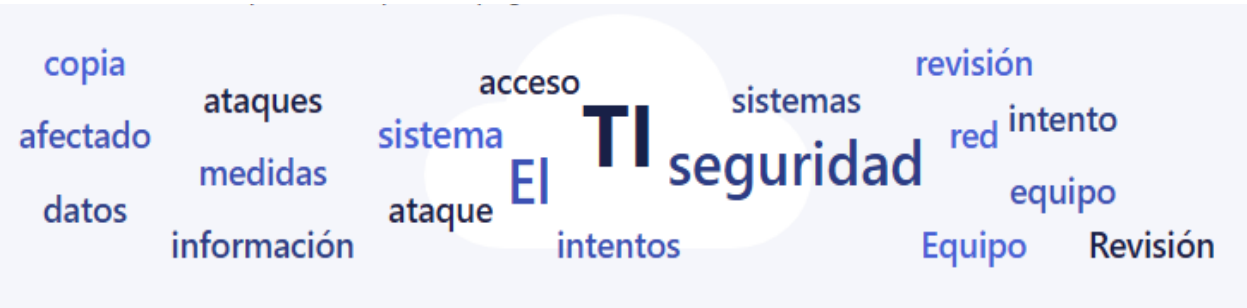


Figura 17 Como se manejó la situación.
Fuente: Elaboración Propia.

La pregunta 5 busca conocer las acciones concretas que las empresas tomaron ante incidentes de ciberseguridad. Al analizar la nube de palabras, podemos inferir lo siguiente:

1. **"Seguridad"** y "**TI**": como respuestas predominantes: El hecho de que estas 2 palabras sean las más frecuentes (con **32 y 43 encuestados** respondiendo así) indica que, para muchas empresas, la respuesta a un incidente se centra en reforzar o revisar sus medidas de seguridad existentes, a esto se le puede implicar una variedad de acciones, como actualizar software, implementar nuevos firewalls, o capacitar al personal.
2. Acciones Clave Reveladas por las Palabras:
    a. "**Sistema**" y "**Red**": Indican que las acciones se centran en proteger y restaurar la infraestructura tecnológica.
    b. "**Datos**" e "**Información**": Subrayan la prioridad de salvaguardar los activos de información.
    c. "**Ataque**" e "**Intentos**": Confirman la presencia de incidentes y la necesidad de respuestas efectivas.
    d. "**Medidas**" y "**Acceso**": Señalan la implementación de controles y acciones específicas.
    e. "**Copia**": Destaca la importancia de las copias de seguridad en la recuperación.
    f. "**Revisión**" y "**Equipo**": Implican la realización de análisis y la participación de equipos especializados.
    g. "**Afectado**": Indica que los incidentes han tenido un impacto en los sistemas.

La nube de palabras refleja que las empresas responden a los incidentes de ciberseguridad mediante una combinación de acciones técnicas (protección de sistemas y redes, recuperación de

datos) y organizativas (revisión de políticas, capacitación). Con la alta frecuencia de "**seguridad**" sugiere que muchas empresas consideran que la mejor respuesta es fortalecer sus defensas para prevenir futuros ataques.

Pregunta 6

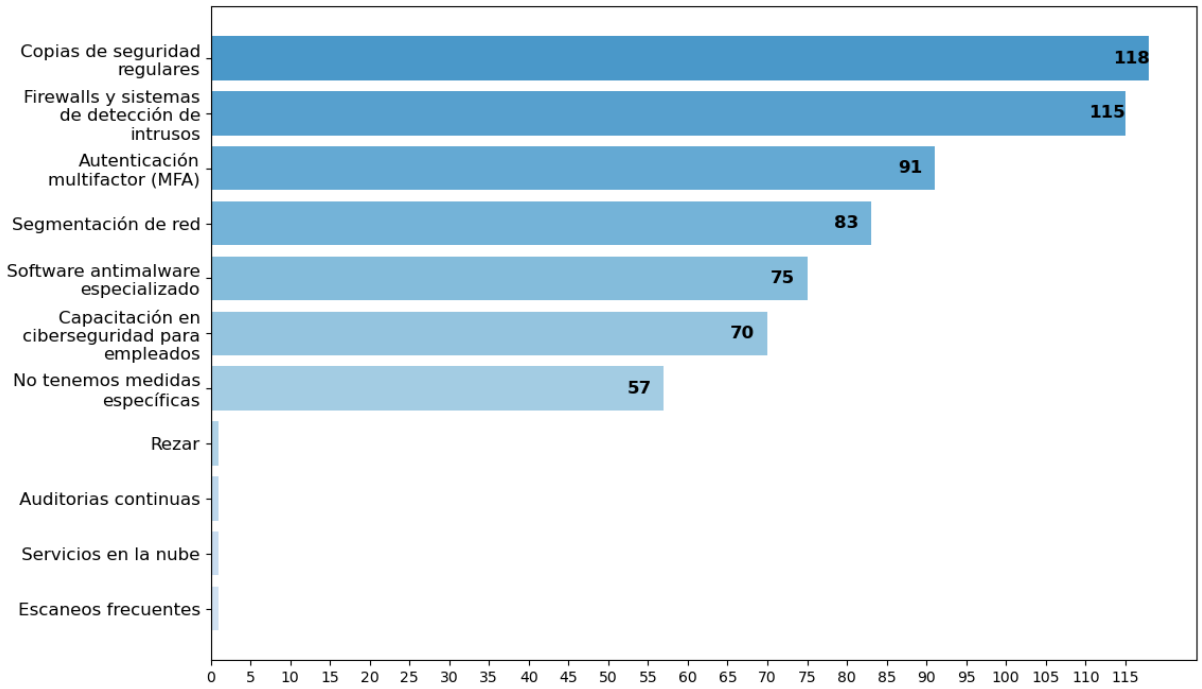


Figura 18 Medidas Preventivas Utilizadas
Fuente: Elaboración Propia.

Los resultados reflejan que las estrategias de prevención de ransomware varían entre las empresas encuestadas. Las medidas más utilizadas son las "**copias de seguridad regulares**" con (**118 respuestas)** y los "**firewalls/sistemas de detección de intrusos**", con (**115 respuestas)**, lo que indica que muchas empresas priorizan la protección de datos y el monitoreo del tráfico para detectar posibles amenazas.

La "**autenticación multifactor (MFA)**" es implementada por (**91 empresas)**, una cifra considerable que resalta la creciente adopción de este mecanismo para fortalecer el acceso a sistemas críticos. Asimismo, (**75 empresas)** utilizan "**software antimalware especializado**", lo que demuestra una conciencia sobre la importancia de herramientas dedicadas a la detección y eliminación de amenazas.

Sin embargo, "**la segmentación de red**" con (**83 respuestas**) y la "**capacitación en ciberseguridad para empleados"** con (**70 respuestas**), esto indica que no son adoptadas en la misma medida que las otras estrategias, a pesar de ser elementos clave en la defensa contra ataques de ransomware. Lo encontrado sugiere que aún existe una brecha en la implementación de prácticas que podrían reducir significativamente la propagación de ataques dentro de las organizaciones.

Un dato preocupante es que (**57 empresas)** indicaron que "**no cuentan con medidas específicas de protección**", lo que las hace altamente vulnerables ante el ransomware. Este hallazgo enfatiza la necesidad de reforzar la cultura de seguridad en el ámbito empresarial hondureño y promover la adopción de estrategias de prevención más completas.

Finalmente, solo (**4 empresas)** reportaron utilizar "**otras medidas**", lo que indica que la mayoría de las organizaciones dependen de prácticas estándar sin innovar en enfoques adicionales de protección. Esto subraya la importancia de diversificar y actualizar continuamente las estrategias de ciberseguridad para enfrentar un panorama de amenazas en constante evolución.

Pregunta 7

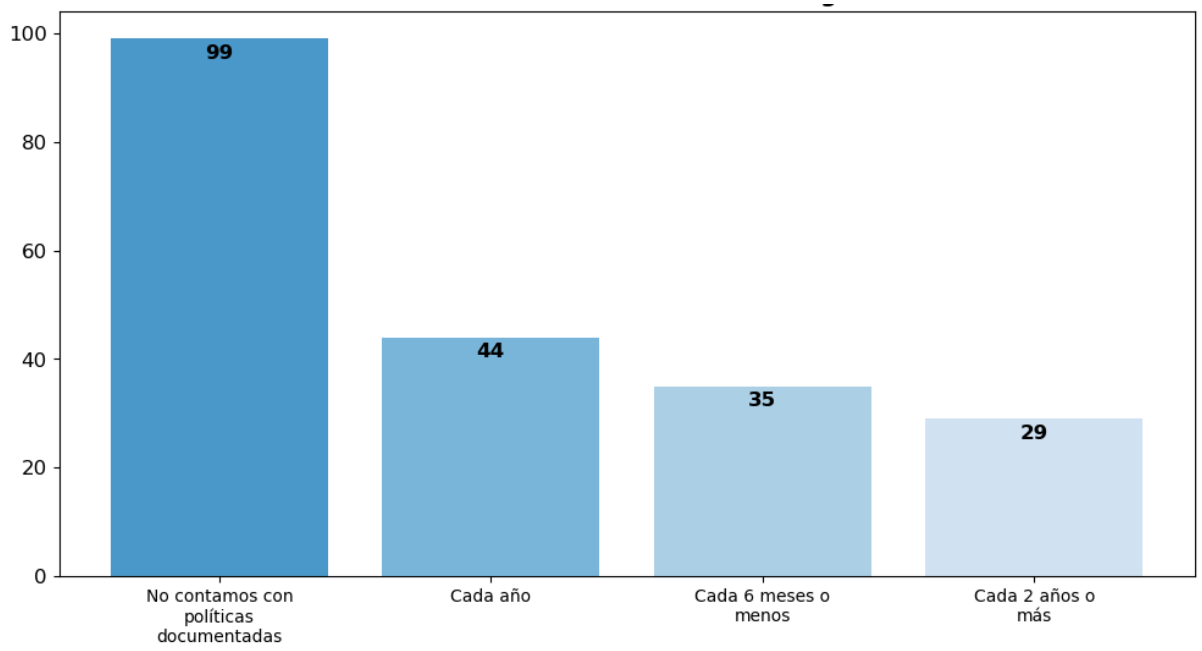


Figura 19 Actualización de Políticas de Ciberseguridad
Fuente: Elaboración Propia.

Los resultados evidencian una falta generalizada de formalización y actualización de políticas de ciberseguridad en muchas empresas hondureñas. Un hallazgo alarmante es que (**99 empresas)** indicaron que **"no cuentan con políticas documentadas"**, lo que representa una gran vulnerabilidad, ya que la ausencia de lineamientos claros dificulta la respuesta ante amenazas y limita la implementación de buenas prácticas.

Por otro lado, (**44 empresas) "actualizan sus políticas cada año"**, lo que indica un nivel de compromiso moderado con la ciberseguridad. Sin embargo, considerando la rapidez con la que evolucionan las amenazas cibernéticas, este periodo podría no ser suficiente en algunos casos.

Solo (**35 empresas)** realizan **"actualizaciones cada 6 meses o menos"**, lo que refleja un enfoque proactivo y alineado con prácticas internacionales, donde las revisiones periódicas permiten ajustar estrategias en función de las nuevas amenazas y vulnerabilidades emergentes.

Finalmente, (**29 empresas) "actualizan sus políticas cada dos años o más"**, lo que representa un riesgo considerable, ya que las amenazas evolucionan constantemente y este periodo prolongado puede dejar brechas de seguridad sin atender. En general, los datos sugieren que muchas empresas en Honduras aún no han desarrollado un marco sólido de políticas de ciberseguridad, lo que resalta la necesidad de concientización y adopción de mejores prácticas en el sector empresarial.

Pregunta 8

Los datos recopilados muestran una tendencia clara sobre las acciones prioritarias que las empresas hondureñas tomarían en caso de un ataque de ransomware. A continuación, se presenta el análisis en orden de prioridad según las prioridades de las empresas ante un ataque de ransomware, destacando que la acción más común es aislar los sistemas y contactar a especialistas en ciberseguridad, seguida de la restauración de datos desde copias de seguridad, mientras que pagar el rescate es la opción menos preferida, y aunque la mayoría tiene planes de acción, aún existe un porcentaje que carece de ellos, subrayando la necesidad de fortalecer las capacidades de respuesta y prevención ante incidentes de ciberseguridad:

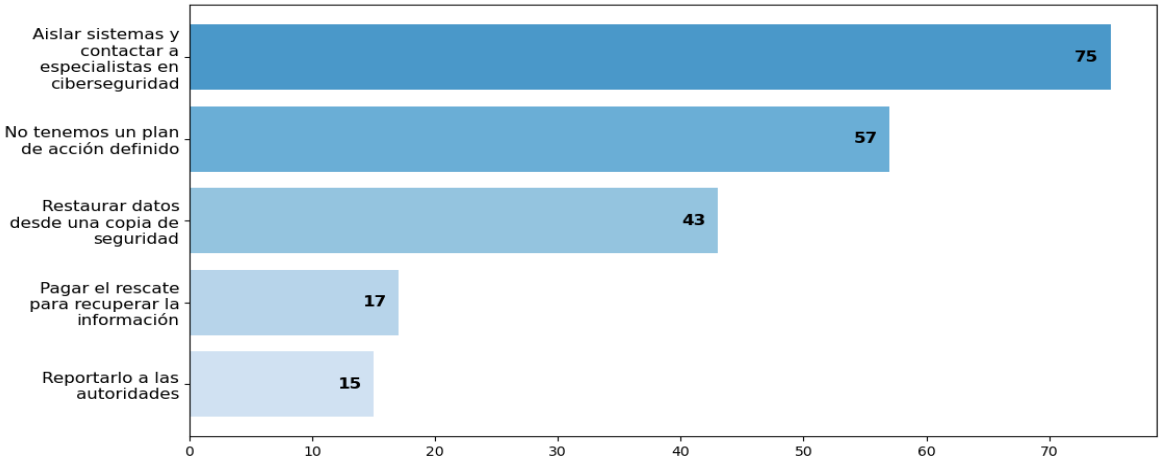


Figura 20 Acciones Como Prioridad 1 Ante Ransomware
Fuente: Elaboración Propia.

Este paso es considerado de alta prioridad, con (**75 empresas**) colocándolo en primer lugar y un segundo con (**43 empresas**) el "**restaurar datos**", pero "**Aislar los sistemas infectados"** es una medida crítica para evitar la propagación del ransomware dentro de la red empresarial, mientras que contactar a especialistas permite una respuesta más técnica y controlada. No obstante, esto lo que indica es que algunas empresas idea de contar con protocolos claros para la contención del ataque.

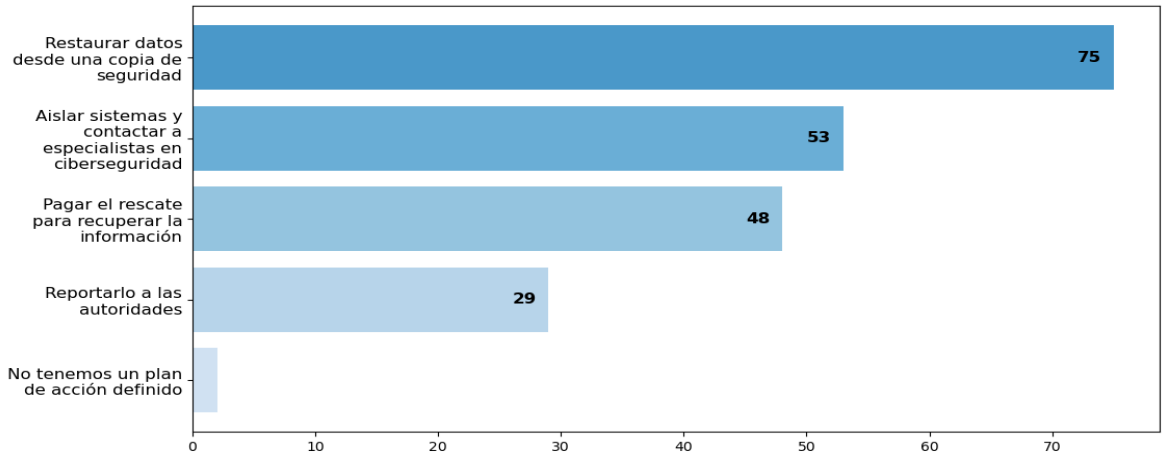


Figura 21 Acciones Como Prioridad 2 Ante Ransomware
Fuente: Elaboración Propia.

La opción más priorizada por las empresas encuestadas es restaurar los datos desde una copia de seguridad, con un 36% de respuestas en primera prioridad y un 32% en segunda prioridad. Esto indica que una gran parte de las empresas cuenta con respaldos de información y considera esta acción como la más efectiva para recuperar sus operaciones sin recurrir al pago del rescate.

Sin embargo, un 9% la coloca en cuarta prioridad y un 2% en quinta, lo que sugiere que algunas organizaciones pueden no estar seguras sobre la viabilidad o accesibilidad de sus respaldos en caso de un ataque.

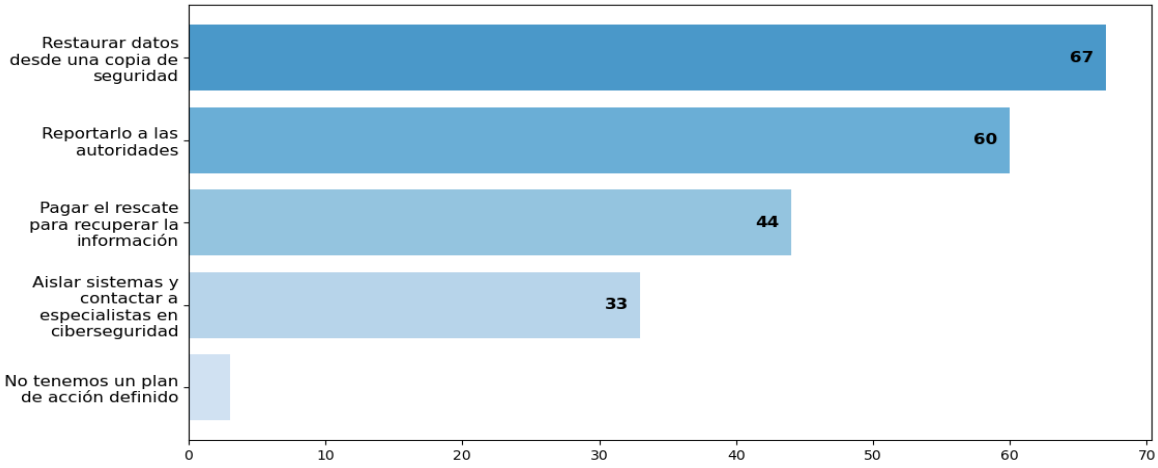


Figura 22 Acciones Como Prioridad 3 Ante Ransomware
Fuente: Elaboración Propia.

Esta opción no es considerada una prioridad para la mayoría de las empresas, ya que solo un 7% la clasifica en primer lugar y un 14% en segundo. La mayoría la ubica en tercer (29%), cuarto (24%) o quinto lugar (26%), lo que indica que existe una falta de confianza en las instituciones gubernamentales o una percepción de que reportar el incidente no contribuye directamente a la recuperación de la información.

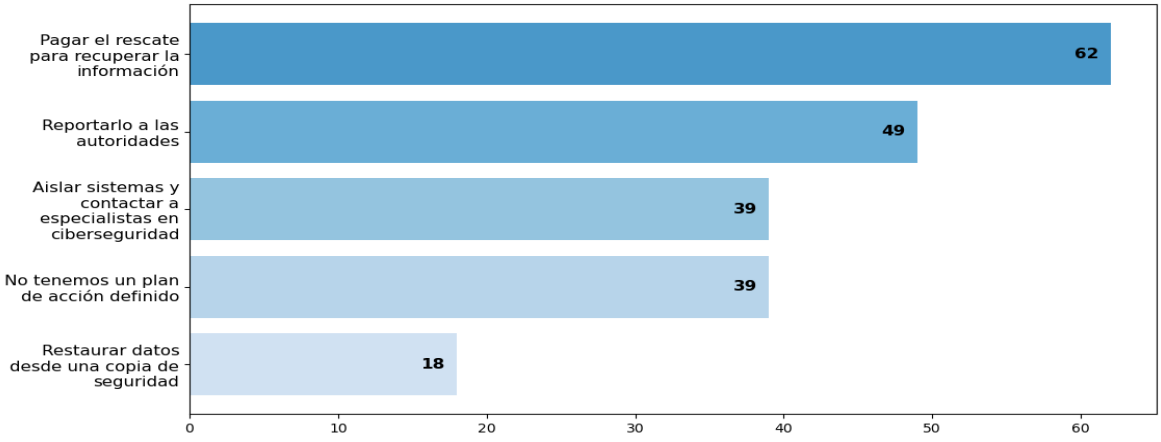


Figura 23 Acciones Como Prioridad 4 Ante Ransomware
Fuente: Elaboración Propia.

A pesar de que el "**pago del rescate**" no es una práctica recomendada por los expertos en

ciberseguridad, un 8% ósea (**62 empresas**), lo considera su primera opción y un 23% su segunda. Esto podría deberse a la falta de respaldos adecuados o a la necesidad de recuperar datos críticos rápidamente. Sin embargo, la mayoría de las empresas lo ubica en cuarta (30%) o quinta prioridad (17%), lo que demuestra que una gran parte de las organizaciones evita esta acción, probablemente debido al riesgo de que el pago no garantice la recuperación de los archivos.

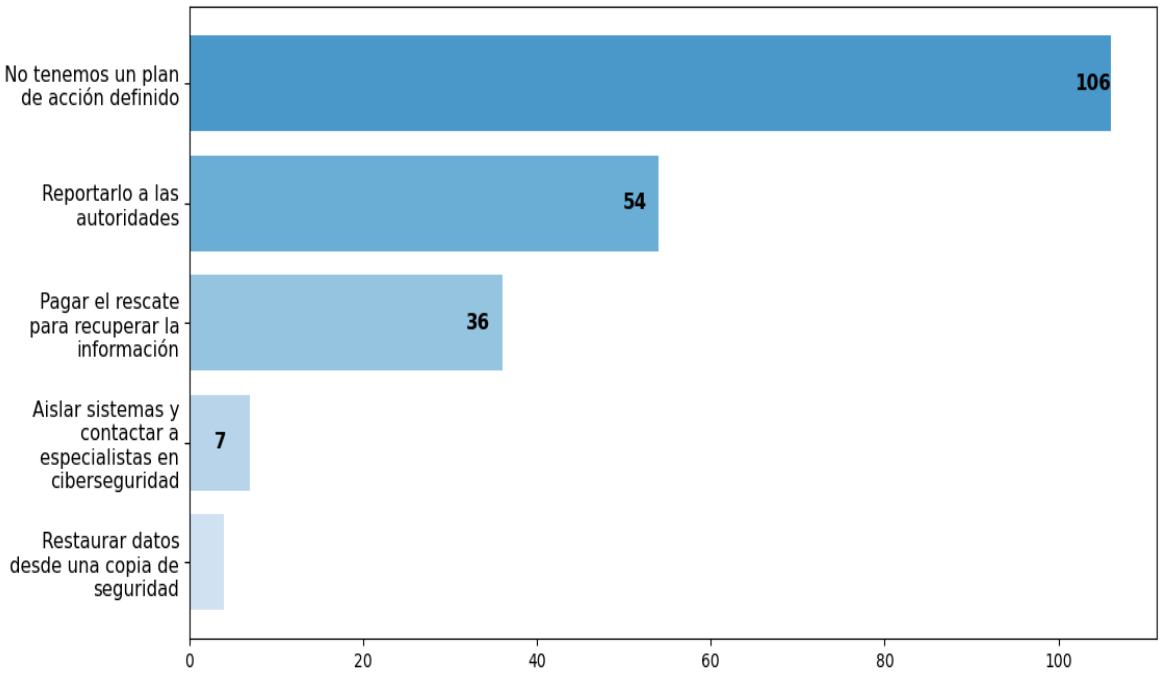


Figura 24 Acciones Como Prioridad 5 Ante Ransomware
Fuente: Elaboración Propia.

El hallazgo más preocupante es que 51%, (**106 empresas**) indicaron "**no contar con un plan de acción definido**", aún existe un porcentaje que carece de ellos, subrayando la necesidad de fortalecer las capacidades de respuesta y prevención ante incidentes de ciberseguridad, lo que las deja completamente expuestas ante un ataque de ransomware. Además, un 19% la coloca en cuarta prioridad esta opcion, lo que sugiere que muchas organizaciones aún no han establecido estrategias claras para responder ante un incidente de esta magnitud.

Pregunta 9

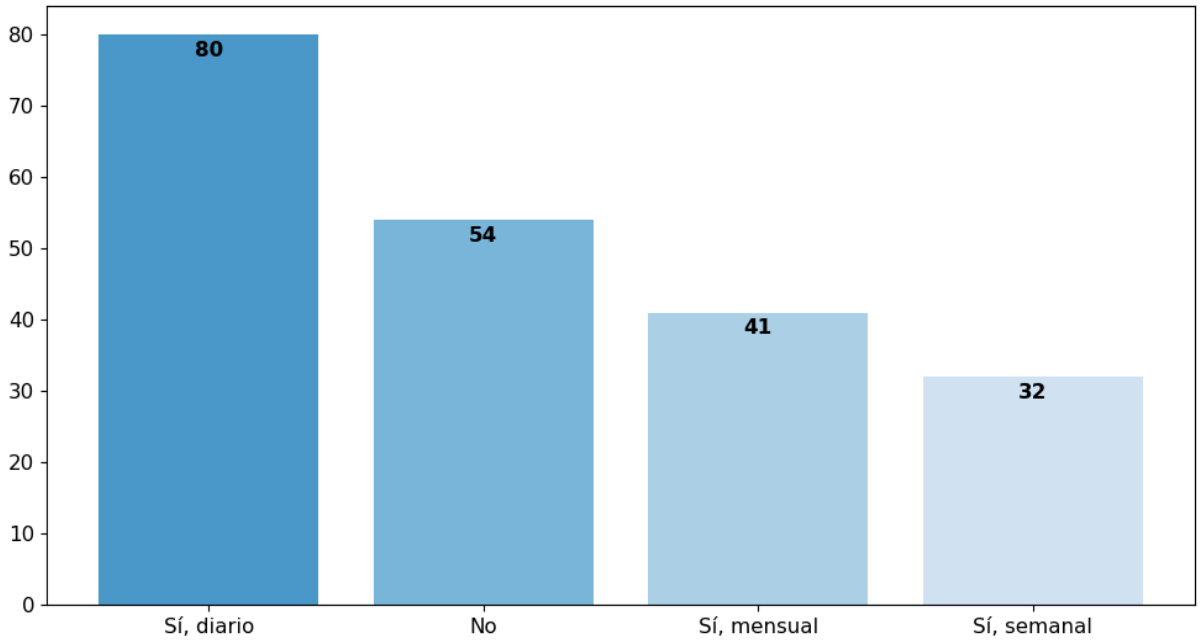


Figura 25 Uso de Sistemas de Respaldo
Fuente: Elaboración Propia.

Los resultados indican que la mayoría de las empresas encuestadas implementan sistemas de respaldo de información con distinta frecuencia. Un 39% realiza "**copias de seguridad diariamente**" (**80 empresas**), lo que demuestra una estrategia sólida de protección de datos. Un 15% lo hace de forma "**semanal**" (**32 empresas**), mientras que un 20% opta por "**respaldos mensuales**" (**41 empresas**), lo que podría aumentar su exposición a la pérdida de información en caso de un ciberataque o falla crítica. Y un 26% que son (**54 empresas**) "**no cuenta con un sistema de respaldo regular**", lo que representa un riesgo significativo ante incidentes de seguridad como ataques de ransomware. Estos hallazgos resaltan la importancia de fortalecer las estrategias de respaldo en las organizaciones para garantizar la continuidad operativa y la recuperación de datos.

Pregunta 10

El análisis de los resultados revela que una gran proporción de las empresas carece de un plan de contingencia formal ante ataques de ransomware. Son (**97 empresas**) que "**no cuenta con un plan documentado"**, lo que las deja vulnerables ante incidentes de seguridad.

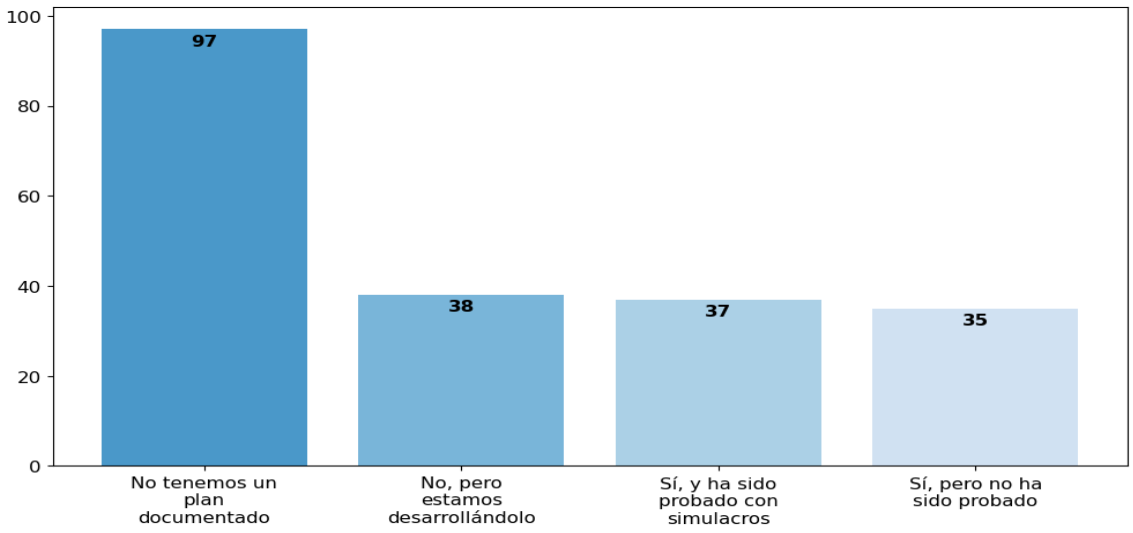


Figura 26 Disponibilidad de un Plan de Contingencia
Fuente: Elaboración Propia.

Y (**38 empresas**) está en "**proceso de desarrollar uno**", lo que indica una creciente conciencia sobre la importancia de la preparación, aunque aún sin medidas efectivas implementadas. Por otro lado (**35 empresas**) "**tiene un plan de contingencia**", pero no lo ha probado, lo que podría limitar su efectividad en un escenario real. Solo (**37 empresas**) "**ha documentado y probado su plan a través de simulacros**", demostrando un nivel de preparación más avanzado. Estos hallazgos subrayan la necesidad de fortalecer la planificación y prueba de planes de respuesta para minimizar el impacto de ataques de ransomware en las organizaciones.

Pregunta 11

Los resultados reflejan que las principales barreras para mejorar la ciberseguridad en las empresas hondureñas son el "**desconocimiento de los riesgos**" con (**118 respuestas**), que representa el 26% y que es preocupante esta cantidad, ya que el desconocimiento sobre amenazas como el ransomware hace que muchas organizaciones no prioricen la inversión en seguridad hasta que sufren un ataque, lo que las deja altamente expuestas. También la "**falta de presupuesto**" con (**101 respuestas**) ósea el 23%, lo que limita la adquisición de herramientas avanzadas, la capacitación del personal y la contratación de expertos y la "**escasez de personal especializado**" (**92 respuestas**), mientras haya esta escasez de profesionales especializados en ciberseguridad dificulta la implementación de estrategias efectivas para detectar, prevenir y mitigar ataques.

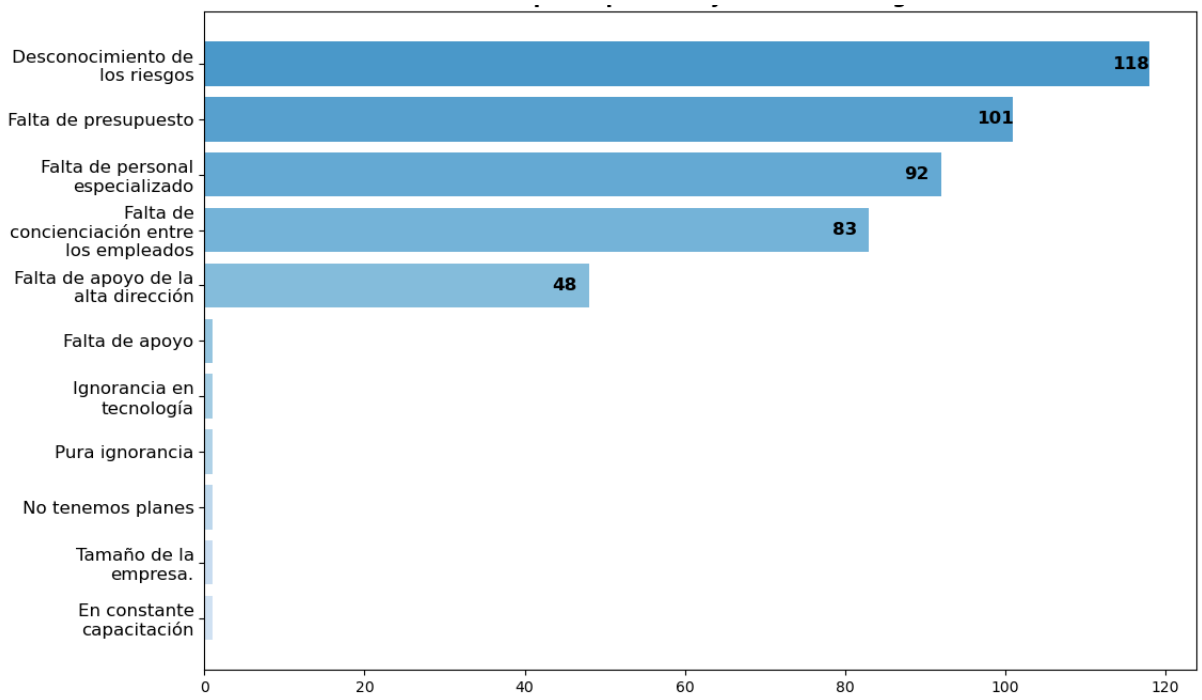


Figura 27 Barreras que Impiden Mejorar la Ciberseguridad
Fuente: Elaboración Propia.

Además, con (**83 respuestas**) que indicaron que la "**falta de concienciación entre los empleados**", este hallazgo destaca la necesidad urgente de fortalecer la educación en ciberseguridad, asignar presupuestos adecuados, capacitar talento especializado y promover una cultura organizacional que priorice la protección de la información incrementa los riesgos, ya que la ausencia de formación en buenas prácticas facilita la propagación de ataques de phishing e ingeniería social.

La "**falta de apoyo de la alta dirección**" con (**48 respuestas**) también representa un obstáculo, ya que, sin un compromiso claro desde los niveles ejecutivos, los programas de ciberseguridad pueden quedar relegados o recibir recursos insuficientes. Finalmente, un grupo reducido de empresas (**6 respuestas**) mencionó otras barreras, posiblemente relacionadas con infraestructura tecnológica deficiente, falta de normativas locales o dependencia de proveedores externos.

Pregunta 12

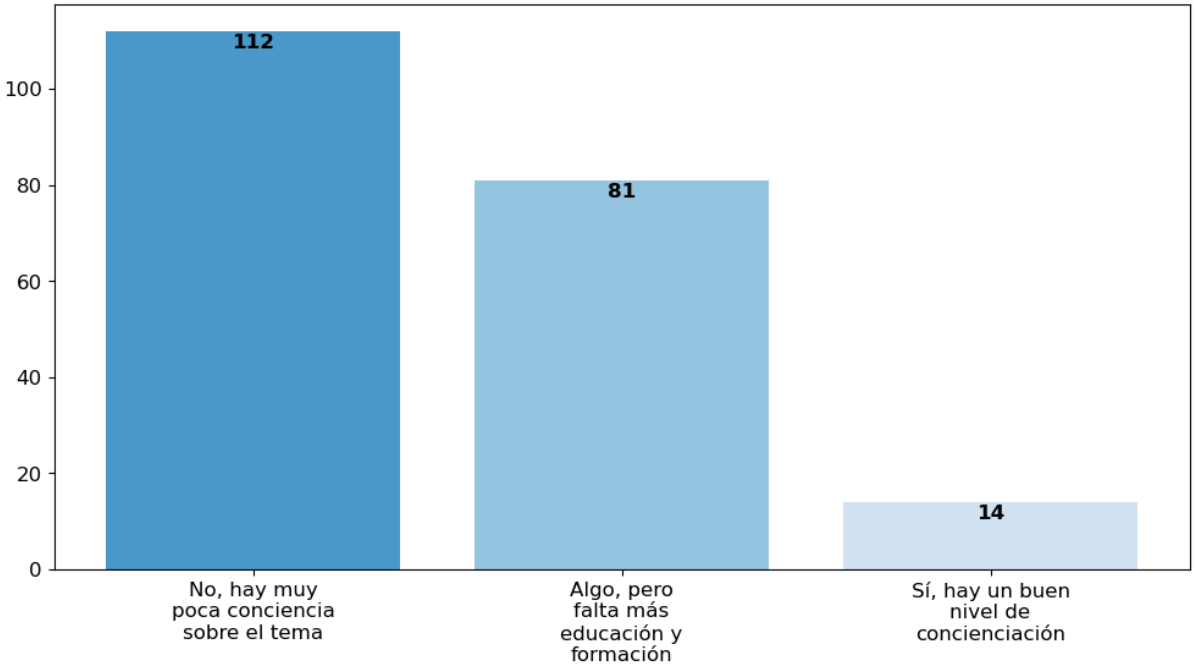


Figura 28 Nivel de Conciencia en Honduras
Fuente: Elaboración Propia.

Los resultados indican que la percepción sobre la concienciación del ransomware en el sector empresarial hondureño es mayoritariamente negativa. (**112 empresas**) lo que equivale a 54% consideran que "**hay muy poca conciencia sobre el tema**", lo que evidencia una falta de preparación en el sector para enfrentar este tipo de amenazas. (**81 empresas)** un 39% reconocen que existe cierto nivel de conocimiento, pero que aún es insuficiente y se requiere más educación y formación en ciberseguridad. Solo (**14 empresas**) que son el 7%, consideran que el nivel de concienciación es adecuado, lo que sugiere que son una minoría las organizaciones que han tomado medidas efectivas en la materia.

Estos resultados reflejan la urgente necesidad de fortalecer la educación y concienciación en ciberseguridad dentro del sector empresarial hondureño, promoviendo capacitación continua, simulaciones de ataques y adopción de mejores prácticas. La falta de conocimiento no solo incrementa la vulnerabilidad de las empresas, sino que también impide la implementación de estrategias preventivas eficaces.

Pregunta 13

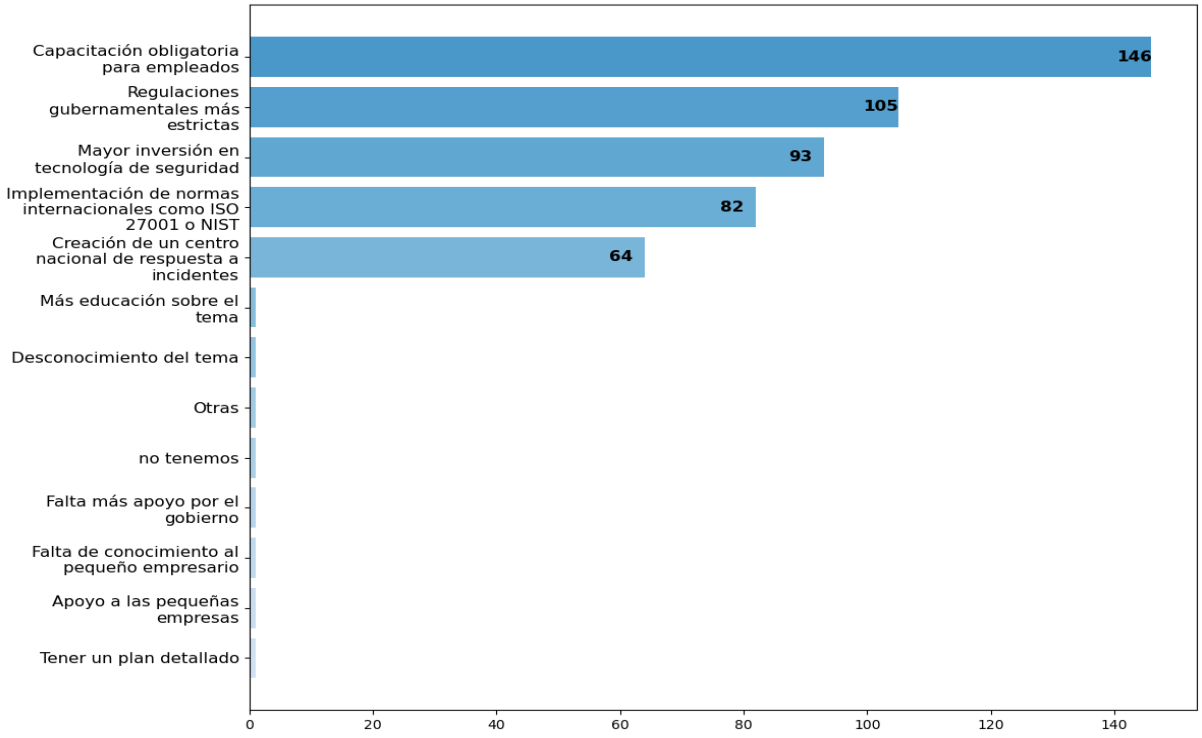


Figura 29 Estrategias para Fortalecer la Ciberseguridad
Fuente: Elaboración Propia.

Los resultados reflejan que las estrategias más valoradas para fortalecer la ciberseguridad en las empresas hondureñas son la "**capacitación obligatoria para empleados**" con (**146 respuestas**) y la "**mayor inversión en tecnología de seguridad**" (**93 respuestas**). Esto indica que la mayoría de los encuestados considera que la formación del personal es clave para reducir vulnerabilidades, especialmente ante amenazas como el ransomware, donde el factor humano es un punto crítico. La inversión en tecnología de seguridad, como firewalls, sistemas de detección de intrusos y soluciones de monitoreo, también es vista como una prioridad para mejorar la protección de las organizaciones.

En tercer lugar, con (**105 respuestas**) señalaron que es necesario contar con "**regulaciones gubernamentales más estrictas**", lo que sugiere que existe una demanda por políticas públicas que obliguen a las empresas a implementar medidas de seguridad más robustas. Además, (**82 empresas**) consideran que la "**adopción de normas internacionales como ISO 27001 o NIST**" es una estrategia clave, lo que demuestra un interés en alinearse con estándares globales de ciberseguridad. La "**creación de un centro nacional de respuesta a incidentes**" con la cantidad

de (**64 respuestas**), también es vista como una estrategia importante, aunque menos prioritaria, mientras que solo 8 empresas indicaron otras medidas no especificadas.

Estos hallazgos resaltan la necesidad de un enfoque integral que combine capacitación, inversión en tecnología, regulación gubernamental y adopción de estándares internacionales para fortalecer la ciberseguridad en Honduras.

Análisis Univariado

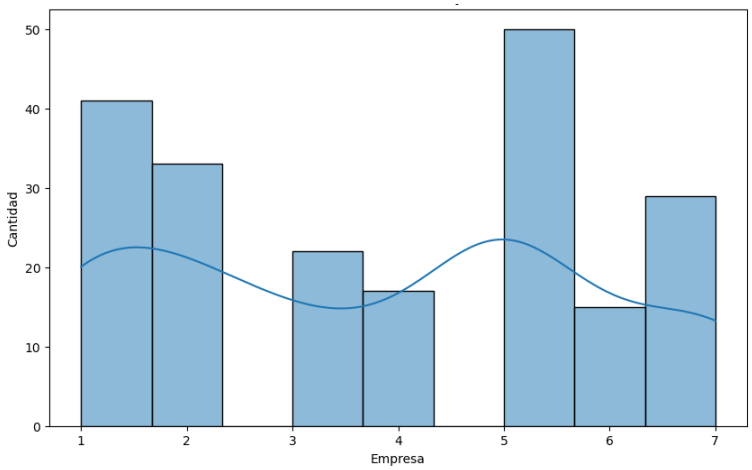


Figura 30 Histograma Empresas
Fuente: Elaboración Propia.

Los resultados muestran una distribución desigual de las empresas encuestadas por sector, con una clara predominancia del sector de TI (5), que cuenta con aproximadamente 50 empresas, sugiriendo un fuerte enfoque en este sector durante la encuesta; le siguen los sectores de Finanzas (1) y Gobierno (2) con una representación significativa de aproximadamente 40 y 33 empresas respectivamente, indicando una relevancia importante de estos sectores en el estudio; los sectores de Educación (3) y Servicio público (4) presentan una representación moderada de aproximadamente 22 y 17 empresas respectivamente, lo que refleja una diversidad en la muestra; finalmente, los sectores de Salud (6) y Otras (7) son los menos representados, con aproximadamente 15 y 29 empresas respectivamente, donde la baja representación del sector salud podría indicar menor participación o interés, mientras que la cantidad en "otras" invita a revisar los sectores que agrupa.

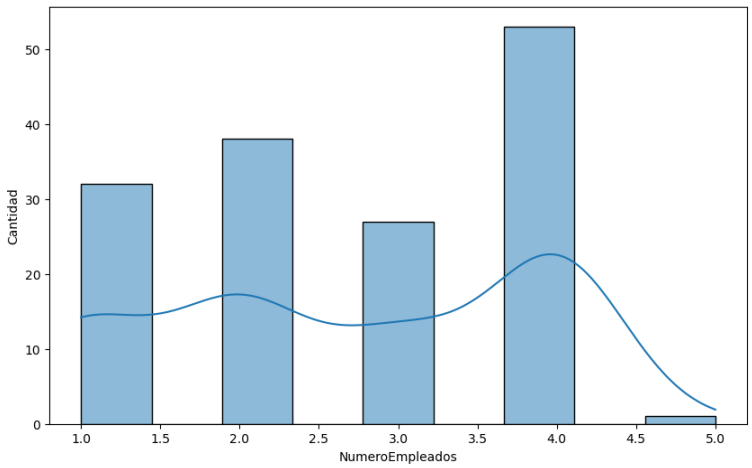


Figura 31 Histograma Número de Empleados
Fuente: Elaboración Propia.

Los resultados muestran una distribución desigual en el tamaño de las empresas encuestadas, con una clara predominancia de aquellas con "Más de 100 empleados" (4), que cuentan con la mayor cantidad de empresas, sugiriendo un fuerte enfoque en este segmento durante la encuesta; le sigue el grupo de empresas "Entre 20 - 50 empleados" (2) con una representación significativa, indicando una relevancia importante de este segmento en el estudio; los grupos de "Entre 1 - 20 empleados" (1) y "Entre 50 - 100 empleados" (3) presentan una representación moderada, lo que refleja una diversidad en la muestra finalmente, estos dos últimos grupos son los menos representados, mientras que la predominancia de empresas grandes invita a considerar las posibles diferencias en necesidades y perspectivas al analizar los resultados generales.

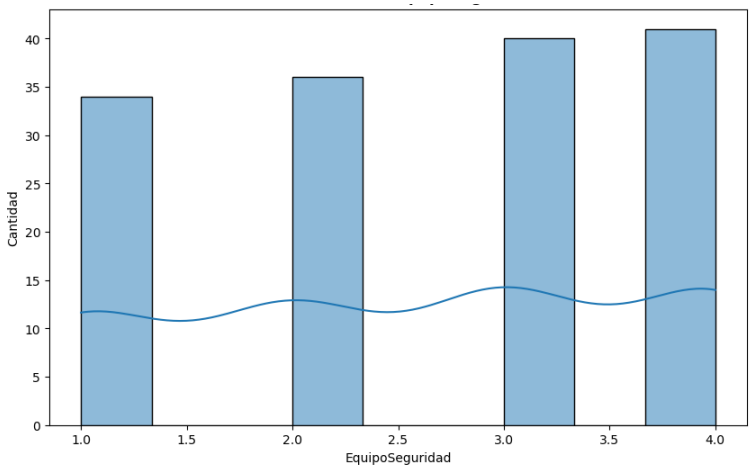


Figura 32 Histograma Equipo de Ciberseguridad
Fuente: Elaboración Propia.

Los resultados revelan una distribución bimodal en la disponibilidad de equipos de

ciberseguridad, donde la mayoría de las empresas encuestadas se agrupa en dos categorías principales: aquellas que "No tienen medidas de ciberseguridad específicas" (4) y aquellas donde "La seguridad es gestionada por el equipo de TI" (3), ambas con una representación similar, lo que indica una falta de especialización en ciberseguridad; por otro lado, se observa una representación similar pero menor en las categorías de empresas que "Sí tercerizan el servicio" (2) y aquellas que cuentan con "Personal especializado interno" (1), sugiriendo una diversidad en las estrategias de ciberseguridad, pero resaltando la necesidad de mejoras significativas en la implementación de medidas especializadas para la mayoría de las empresas.

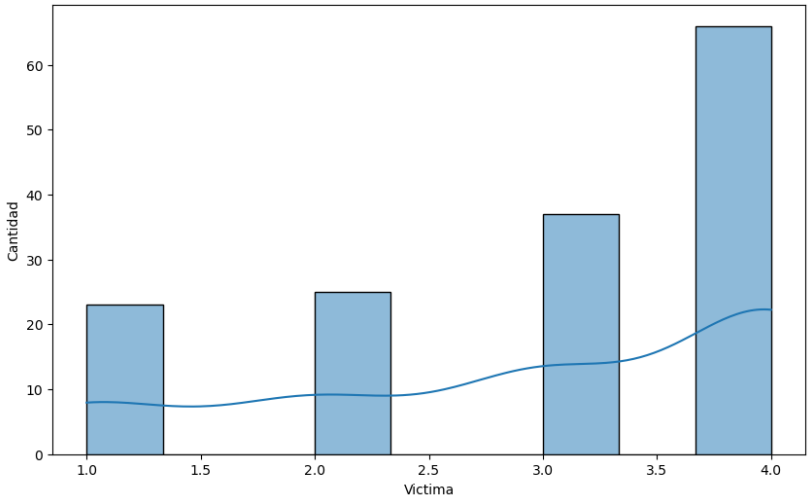


Figura 33 Histograma de Victimas de Ransomware
Fuente: Elaboración Propia.

Los resultados muestran una distribución asimétrica en la experiencia de las empresas como víctimas de incidentes de seguridad, donde la mayoría de las empresas encuestadas se agrupa en la categoría "No" (4), lo que indica que no han sido víctimas; sin embargo, un número significativo de empresas reporta haber detectado intentos de ataque (3), lo que sugiere una conciencia de las amenazas; mientras tanto, las categorías de empresas que han sido víctimas, ya sea "Una sola vez" (2) o "En más de una ocasión" (1), tienen una representación menor, aunque aún relevante, subrayando el riesgo continuo de incidentes de seguridad a pesar de la predominancia de empresas que no han sido víctimas directas.

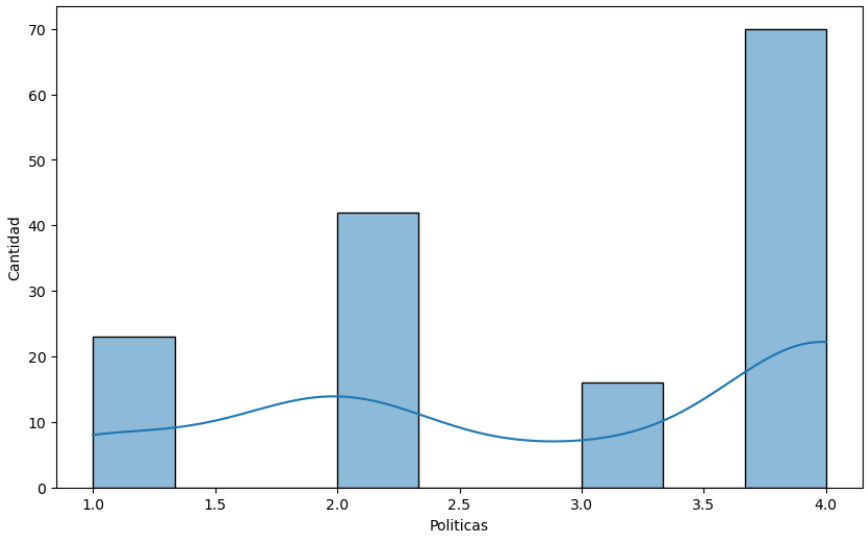


Figura 34 Histograma de Políticas
Fuente: Elaboración Propia.

Los resultados muestran una distribución asimétrica en la frecuencia de actualización de políticas de seguridad, donde la mayoría de las empresas encuestadas se agrupa en la categoría "No contamos con políticas documentadas" (4), lo que indica una falta significativa de políticas formales; le sigue una cantidad considerable de empresas que actualizan sus políticas "Cada año" (2), sugiriendo una conciencia de la necesidad de revisión periódica; mientras tanto, las categorías de actualización "Cada 6 meses o menos" (1) y "Cada 2 años o más" (3) tienen una representación menor, lo que subraya la necesidad de una mayor formalización y actualización regular de políticas de seguridad para la mayoría de las empresas.

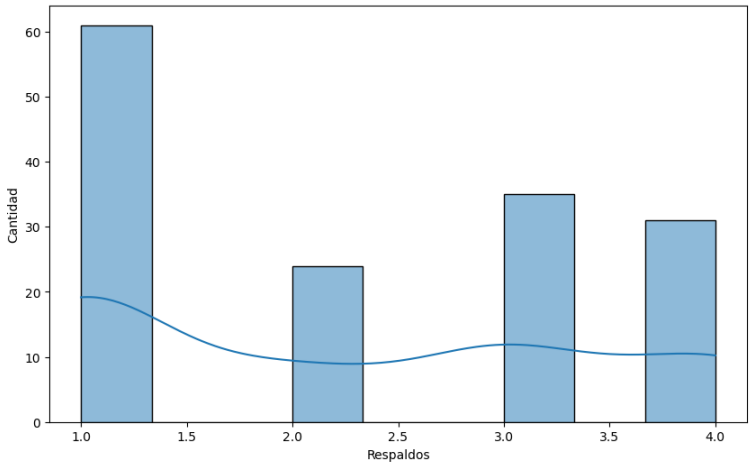


Figura 35 Histograma de Respaldos
Fuente: Elaboración Propia.

Los resultados muestran una distribución asimétrica en la frecuencia de realización de

respaldos de información, donde la mayoría de las empresas encuestadas se agrupa en la categoría "Sí, diario" (1), lo que indica una práctica de respaldo sólida y frecuente; sin embargo, se observa una distribución considerable en las categorías "Sí, mensual" (3) y "No" (4), lo que sugiere que muchas empresas realizan respaldos con menor frecuencia o no los realizan en absoluto, representando un riesgo significativo de pérdida de datos; mientras tanto, la categoría "Sí, semanal" (2) tiene una representación menor, lo que subraya la necesidad de mejorar las prácticas de respaldo en muchas empresas, especialmente en aquellas que realizan respaldos con menor frecuencia o no los realizan.

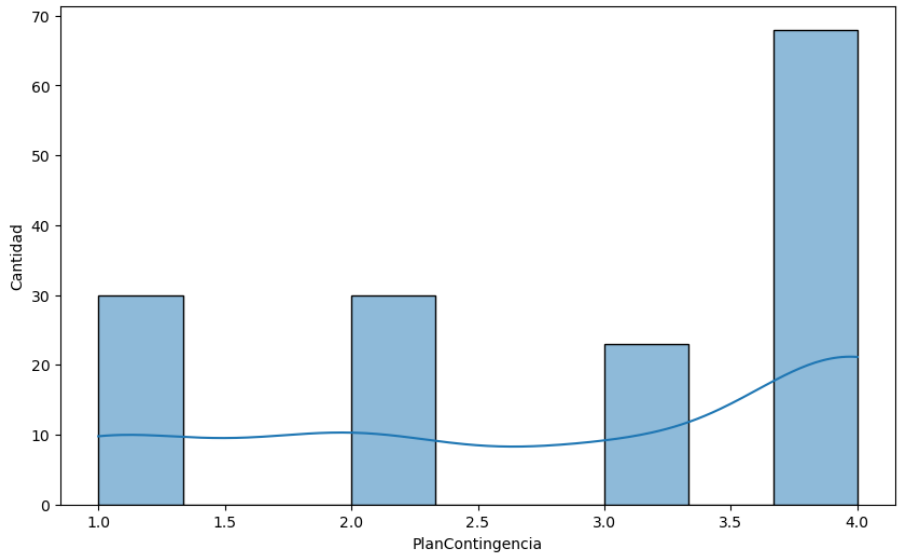


Figura 36 Histograma de Plan de Contingencia
Fuente: Elaboración Propia.

Los resultados muestran una distribución asimétrica en la disponibilidad y estado de los planes de contingencia, donde la mayoría de las empresas encuestadas se agrupa en la categoría "No tenemos un plan documentado" (4), lo que indica una falta significativa de planes formales; le siguen las categorías "Sí, y ha sido probado con simulacros" (1) y "Sí, pero no ha sido probado" (2), ambas con una representación similar y moderada, sugiriendo una diversidad en el desarrollo de planes; mientras tanto, la categoría "No, pero estamos desarrollándolo" (3) tiene una representación menor, lo que subraya la necesidad de una mayor formalización y prueba de planes de contingencia para la mayoría de las empresas, especialmente aquellas que carecen de documentación o no han realizado simulacros.

Análisis Bivariado

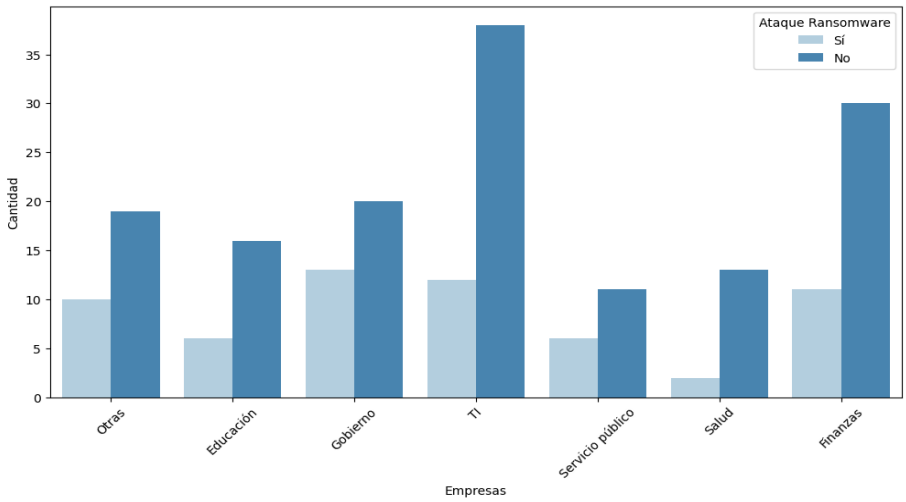


Figura 37 Ataques de Ransomware por Empresa
Fuente: Elaboración Propia.

El gráfico revela que el sector de Tecnología de la Información (TI) es el más afectado por ataques de ransomware, con una cantidad significativamente mayor de empresas que han sufrido ataques en comparación con otros sectores, seguido por el sector de Finanzas, que también muestra una vulnerabilidad considerable; mientras tanto, los sectores de Educación, Gobierno, Servicio público y Salud muestran una menor incidencia de ataques, aunque todos los sectores son vulnerables, subrayando la necesidad de implementar medidas de seguridad sólidas en todas las empresas, independientemente de su sector.

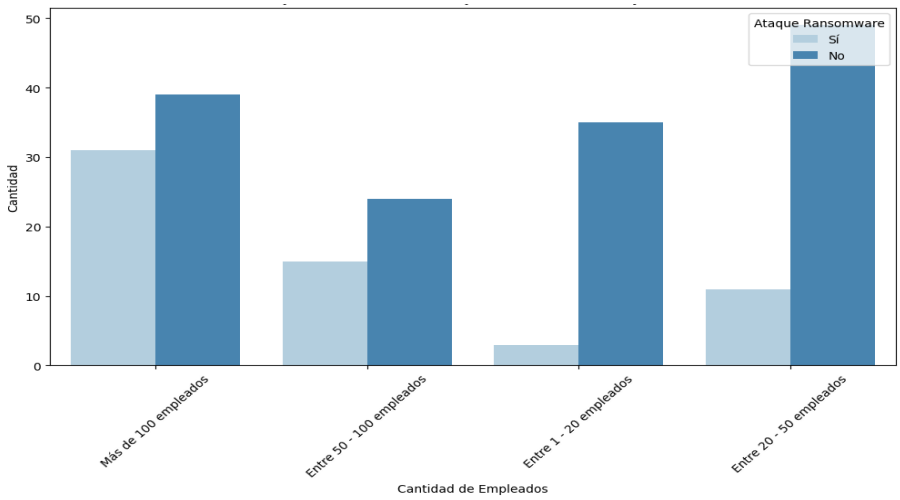


Figura 38 Ataques de Ransomware por Cantidad de Empleados
Fuente: Elaboración Propia.

El gráfico revela una clara tendencia de vulnerabilidad a ataques de ransomware en función del tamaño de la empresa, donde las empresas con "**Más de 100 empleados**" y "**Entre 20-50 empleados**" son las más afectadas, indicando que las empresas grandes y medianas son objetivos primordiales para los ciberdelincuentes, posiblemente debido a la mayor cantidad de datos y recursos que manejan; por otro lado, las empresas con "**Entre 1-20 empleados**" son las menos afectadas, lo que sugiere un menor interés por parte de los atacantes, aunque no exime a estas empresas de la necesidad de medidas de seguridad; en general, se observa una diferencia notable en la proporción de empresas que han sufrido ataques en comparación con las que no en las categorías de empresas grandes y medianas, subrayando la importancia de implementar medidas de seguridad sólidas en todas las empresas, independientemente de su tamaño.

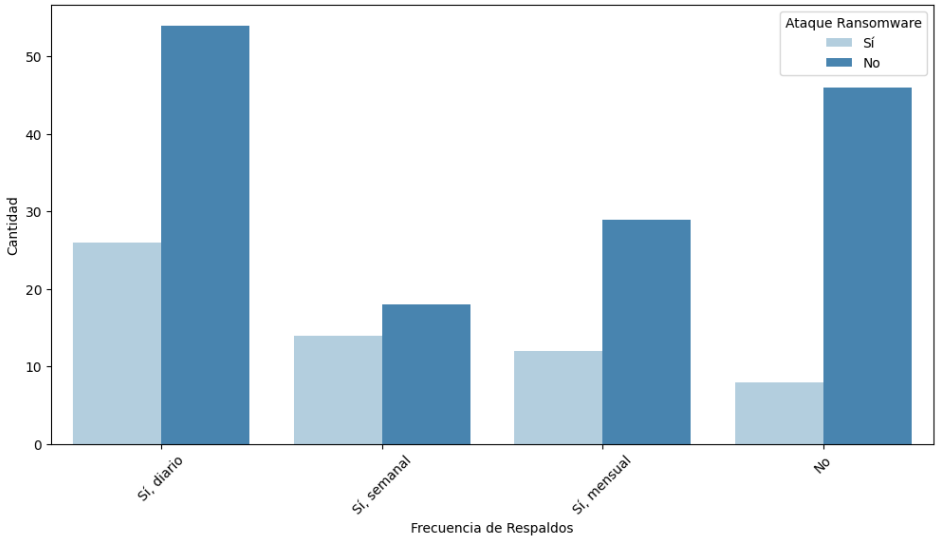


Figura 39 Ataques de Ransomware por Frecuencia de Respaldos
Fuente: Elaboración Propia.

El gráfico revela una aparente paradoja, ya que las empresas que realizan respaldos diarios (**Sí, diario**) muestran la mayor incidencia de ataques de ransomware, sugiriendo que el respaldo por sí solo no garantiza protección y que estas empresas podrían ser objetivos más atractivos para los ciberdelincuentes; mientras tanto, las empresas que realizan respaldos semanales y mensuales (**Sí, semanal y Sí, mensual**) reportan una menor incidencia de ataques, pero incluso aquellas que no realizan respaldos (**No**) experimentan una cantidad significativa de ataques, lo que subraya la necesidad de complementar las prácticas de respaldo con otras medidas de seguridad y mitigar el riesgo en empresas que carecen de respaldos.

Correlación Entre Variables

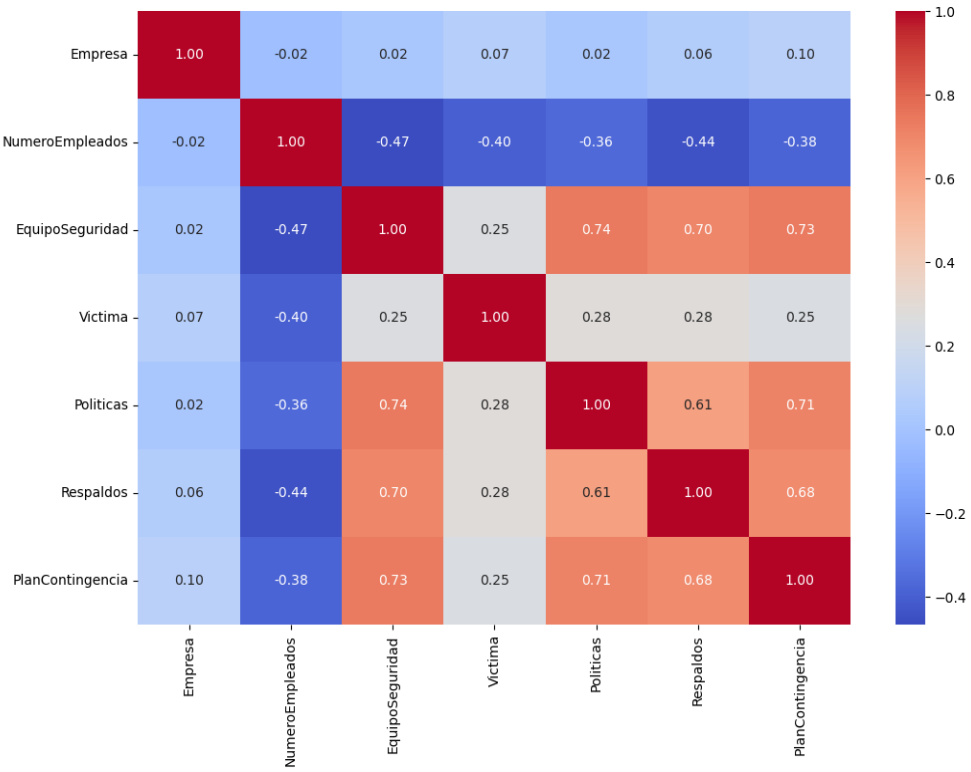


Figura 40 Matriz de Correlación
Fuente: Elaboración Propia.

La matriz de correlación revela que la presencia de un equipo de ciberseguridad especializado tiene una fuerte correlación positiva con la implementación de políticas de seguridad actualizadas, respaldos de información frecuentes y un plan de contingencia documentado, sugiriendo que la inversión en seguridad especializada fomenta prácticas de seguridad robustas; por otro lado, el número de empleados muestra una correlación negativa moderada con las mismas variables de seguridad, indicando que las empresas más grandes podrían descuidar estas prácticas; la variable "Victima" muestra una correlación positiva débil con las prácticas de seguridad, sugiriendo que las empresas tienden a mejorar sus medidas después de sufrir incidentes; finalmente, las correlaciones entre "Empresa" y otras variables son débiles, lo que sugiere que el sector empresarial tiene poca influencia en las prácticas de seguridad.

4.2 INFORME DE PROCESO DE RECOLECCIÓN DE DATOS

4.2.1 DESCRIPCIÓN DEL PROCESO

El proceso de recolección de datos se llevó a cabo mediante una encuesta digital dirigida a

empresas de Honduras, enfocándose en ciberseguridad y ransomware. Este proceso incluyó cuatro etapas:

1. Preparación: Diseño del cuestionario en base a las variables previamente definidas. Para garantizar la claridad y relevancia de las preguntas, el cuestionario fue sometido a un proceso de validación que incluyó una revisión por dos expertos en ciberseguridad y dos gerentes del área de TI. Además, se realizó una prueba piloto con un grupo reducido de participantes, lo que permitió identificar y corregir posibles ambigüedades antes de la distribución masiva.
2. Distribución: Envío de la encuesta a través de correos electrónicos y servicios de mensajería instantánea.
3. Recopilación: Recolección y almacenamiento de las respuestas en un archivo CSV para su posterior análisis en Python.
4. Control de Calidad: Revisión de las respuestas para detectar inconsistencias o posibles sesgos en los datos. Se verificó que las respuestas provinieran de profesionales del sector empresarial y que reflejaran información confiable para el análisis.

4.2.2 PARTICIPANTES

La muestra final estará compuesta por 207 participantes, cada uno perteneciente al área de TI de diversas empresas en Honduras, lo que asegura una representación significativa del nivel de conocimiento y preparación ante amenazas cibernéticas como el ransomware. Los participantes incluyen profesionales con distintos niveles de experiencia en ciberseguridad, desde analistas junior hasta gerentes y directores de seguridad informática. Además, se consideró la antigüedad en la empresa como un factor relevante, permitiendo evaluar cómo la experiencia laboral influye en la percepción y aplicación de medidas de protección contra ransomware. Esta diversidad de perfiles proporciona un panorama más completo sobre el estado de la ciberseguridad en el sector empresarial hondureño.

4.2.3 INSTRUMENTOS UTILIZADOS

Se utilizó un cuestionario estructurado con preguntas de selección única y múltiple, centradas en medidas preventivas, experiencias previas con ransomware y acciones prioritarias ante un ataque. El diseño del cuestionario se basó en un análisis exhaustivo de las variables clave

relacionadas con la ciberseguridad y ransomware, asegurando que las preguntas fueran directamente relevantes para los objetivos de la investigación. Para garantizar la claridad y pertinencia de las preguntas, se realizó una revisión exhaustiva con gerentes del área de TI, quienes proporcionaron retroalimentación sobre la redacción y enfoque de cada ítem. Además, se llevó a cabo una prueba piloto con múltiples profesionales del área de TI, lo que permitió identificar posibles ambigüedades y ajustar las preguntas para asegurar que fueran comprensibles y alineadas con el contexto del estudio. Este proceso de diseño y validación ayudó a garantizar la calidad y precisión de la información obtenida a través del cuestionario.

4.2.4 CONSIDERACIONES ÉTICAS

Al inicio de la encuesta, se informó a los participantes que sus respuestas serían anónimas y que los resultados se utilizarían exclusivamente con fines académicos para esta tesis, garantizando así la confidencialidad y el uso responsable de la información proporcionada. Para asegurar la privacidad de los participantes, se implementó un proceso de anonimización de los datos, de manera que no fuera posible identificar a los encuestados ni asociar sus respuestas con información personal. Además, se utilizó un sistema de almacenamiento seguro de los datos, accesible solo para el equipo de investigación, y se garantizó que los datos serían manejados siguiendo los principios éticos y normativas de protección de la privacidad.

4.3 ANÁLISIS INFERENCIAL Y MODELOS APLICADOS

4.3.1 TIPOS DE MODELOS APLICADOS

Con el objetivo de profundizar el análisis de la investigación se seleccionaron los siguientes cuatro modelos:

1. Árbol de decisión
2. Regresión Logística
3. Gradient Boosting
4. Clustering por K-Means

Para Para evaluar el rendimiento de cada modelo, se utilizaron las variables "Empresa", "NumeroEmpleados", "EquipoSeguridad", "Políticas", "Respaldos" y "ExistePlanContingencia", con el propósito de predecir si una empresa fue víctima de un ataque de ransomware. La selección

de estas variables se basó en su relevancia dentro del contexto de ciberseguridad, considerando su influencia en la preparación y capacidad de respuesta ante amenazas cibernéticas.

El conjunto de datos fue dividido en dos partes: el 80% de los registros se utilizó para el entrenamiento de los modelos, mientras que el 20% restante (42 registros) fue empleado para evaluar su desempeño.

4.3.2 VISUALIZACIÓN DE MODELOS

Árbol de Decisión

El modelo de árbol de decisión fue utilizado en esta investigación para identificar los factores más influyentes en la probabilidad de que una empresa haya sido víctima de un ataque de ransomware. Este modelo permite visualizar, de manera estructurada, cómo variables como el número de empleados, la existencia de un equipo de seguridad, la implementación de políticas de ciberseguridad, la realización de respaldos y la disponibilidad de un plan de contingencia impactan en la exposición al ransomware. Su capacidad para segmentar los datos en función de reglas de decisión facilita la identificación de patrones de riesgo y vulnerabilidades, proporcionando información clave para fortalecer la seguridad de las empresas. Ver **anexo 6.**

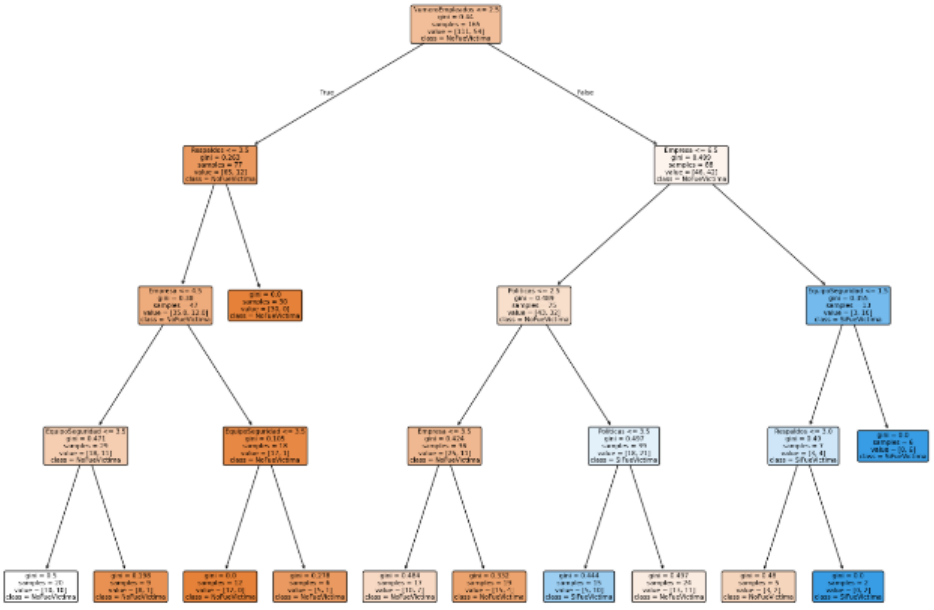


Figura 41 Árbol de decisión
Fuente: Elaboración Propia.

Este árbol de decisión analiza los factores que influyen en la probabilidad de que una empresa sea víctima de ransomware, revelando que las empresas con 20 a 100 empleados y aquellas con respaldos implementados tienen menor riesgo, mientras que la falta de políticas de ciberseguridad y un equipo de seguridad especializado aumenta significativamente la vulnerabilidad, destacando la importancia de invertir en seguridad y concienciar sobre la necesidad de adaptaciones estratégicas según el tamaño y tipo de empresa.

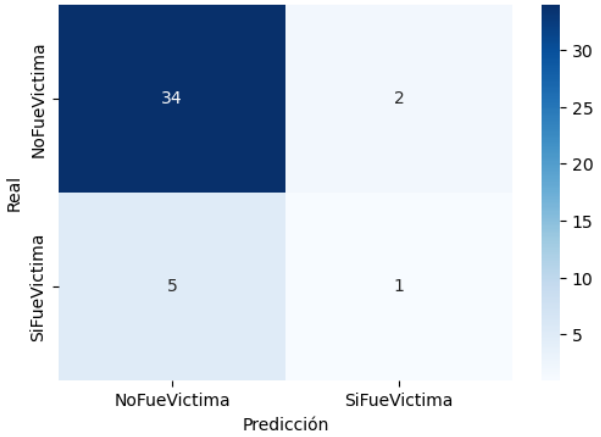


Figura 42 Matriz de Confusión de Árbol de Decisión
Fuente: Elaboración Propia.

La matriz de confusión revela que el modelo de Árbol de Decisión clasificó correctamente a 34 empresas que no fueron víctimas (Verdaderos Negativos) pero erróneamente predijo que 2 empresas no atacadas sí lo fueron (Falsos Positivos). Por otro lado, solo identificó correctamente a 1 empresa que sí fue víctima (Verdadero Positivo), fallando en la predicción para 5 empresas que realmente sufrieron un ataque (Falsos Negativos). En general, el modelo muestra una buena capacidad para identificar a las empresas no afectadas, pero tiene dificultades significativas para detectar correctamente a las empresas que sí fueron víctimas de incidentes de ciberseguridad, lo que sugiere un bajo rendimiento en la identificación de la clase positiva.

Profundidad del Árbol: 4

Precisión del modelo: 83%

Regresión Logística

La regresión logística se aplicó para predecir la probabilidad de que una empresa haya sido víctima de un ataque de ransomware, utilizando como variables predictoras factores clave como

el número de empleados, la existencia de un equipo de seguridad, la implementación de políticas de ciberseguridad, la realización de respaldos y la disponibilidad de un plan de contingencia. Este modelo es adecuado debido a la naturaleza categórica de la variable objetivo, permitiendo estimar la influencia de cada factor en la exposición a ataques de ransomware. Su aplicación proporciona información valiosa para la identificación de vulnerabilidades y la formulación de estrategias preventivas basadas en un análisis estadístico riguroso. Ver **anexo 7.**

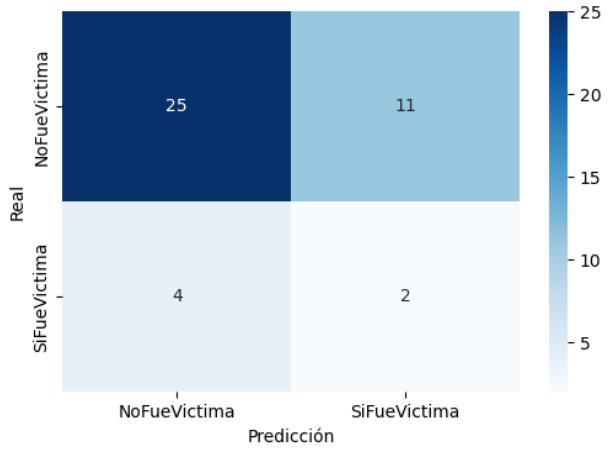


Figura 43 Matriz de Confusión de Regresión Logística
Fuente: Elaboración Propia.

La matriz de confusión muestra que el modelo predice bien a las empresas que no fueron víctimas de ransomware (25 predicciones correctas), pero tiene dificultades para identificar a las que sí lo fueron (solo 2 predicciones correctas), lo que indica un desbalance en los datos y la necesidad de mejorar el modelo para predecir con mayor precisión la clase minoritaria (empresas víctimas) y tomar medidas preventivas efectivas.

Precisión del Modelo: 64.28%

Gradient Boosting

Se recurrió a Gradient Boosting como una técnica de aprendizaje automático supervisado para predecir la probabilidad de ocurrencia de incidentes de ciberseguridad. A diferencia de los métodos no supervisados, Gradient Boosting construye un modelo predictivo combinando secuencialmente múltiples modelos más débiles, corrigiendo los errores de los modelos precedentes para generar una predicción robusta y precisa. Se emplearon como variables predictoras el número de empleados, la existencia de un equipo de seguridad, la implementación

de políticas de ciberseguridad, la realización de respaldos y la disponibilidad de un plan de contingencia. La capacidad de Gradient Boosting para capturar relaciones complejas y no lineales entre estas variables y el riesgo de incidentes permite una evaluación detallada y la identificación de los factores de mayor influencia en la seguridad cibernética empresarial. Los resultados de este modelo predictivo proporcionan información valiosa para la priorización de recursos y la implementación de medidas preventivas dirigidas a reducir la vulnerabilidad ante amenazas cibernéticas. Ver **anexo 8.**

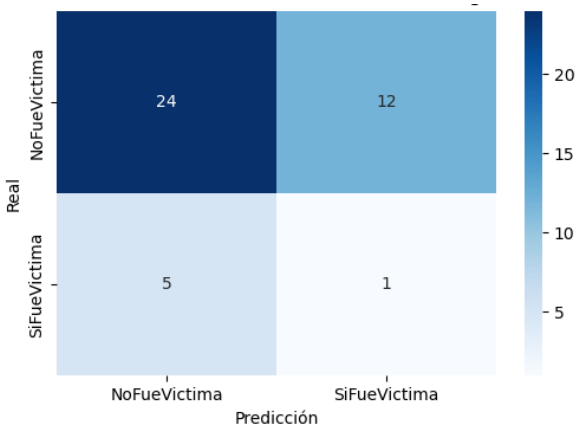


Figura 44 Matriz de Confusión de Gradient Boosting
Fuente: Elaboración Propia.

El modelo de Gradient Boosting muestra un rendimiento moderado en la identificación de empresas que no fueron víctimas (Verdaderos Negativos), pero genera una cantidad considerable de Falsos Positivos, clasificando incorrectamente a muchas empresas no atacadas como si lo hubieran sido. Similar al modelo de Árbol de Decisión, tiene dificultades para identificar correctamente a las empresas que sí fueron víctimas, mostrando un bajo número de Verdaderos Positivos y una cantidad notable de Falsos Negativos. Esto sugiere que el modelo podría estar generando demasiadas alertas innecesarias y, lo que es más preocupante en un contexto de ciberseguridad, no está detectando de manera efectiva a las empresas que realmente sufrieron un ataque.

Precisión del modelo: 59.52%

Comparativa de Modelos Supervisados

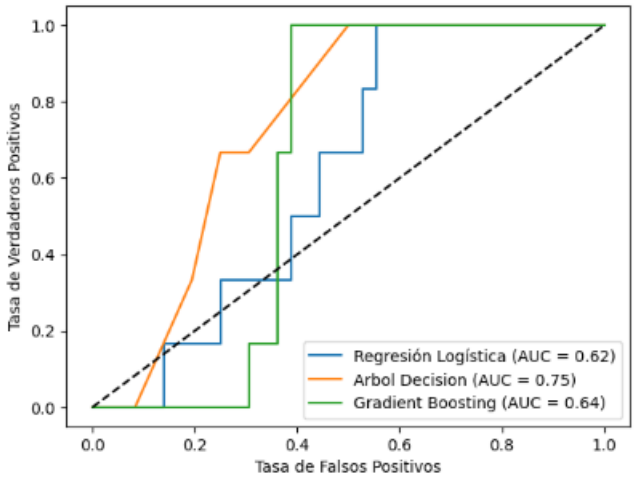


Figura 45 Grafico de Curva ROC
Fuente: Elaboración Propia.

El gráfico de la Curva ROC muestra que el Árbol de Decisión (AUC = 0.75) supera a la Regresión Logística (AUC = 0.62) en la predicción de víctimas de ransomware, logrando una mayor precisión y menor tasa de falsos positivos, lo que lo convierte en el modelo preferible para esta tarea. Ver **anexo 10.**

Tabla 12 Comparativa de Modelos Supervisados

Modelo	Accuracy	AUC-ROC	Precision	Recall
Árbol de decisión	0.762	0.745	0.167	0.167
Gradient Boosting	0.595	0.639	0.077	0.167
Regresión Logística	0.548	0.616	0.190	0.667

Clustering por K-Means

El clustering mediante K-Means fue empleado en esta investigación con el propósito de identificar agrupaciones naturales dentro de los datos en función de variables clave como el número de empleados, la existencia de un equipo de seguridad, la implementación de políticas de ciberseguridad, la realización de respaldos y la disponibilidad de un plan de contingencia. A diferencia de los modelos supervisados, este enfoque permite descubrir patrones ocultos sin necesidad de una variable objetivo, predefinida, facilitando la segmentación de las empresas según

su nivel de exposición y preparación ante ataques de ransomware. La aplicación de K-Means contribuye a la identificación de grupos con características similares, proporcionando información valiosa para diseñar estrategias de ciberseguridad más efectivas y adaptadas a las necesidades específicas de cada segmento empresarial. Ver **anexo 9.**

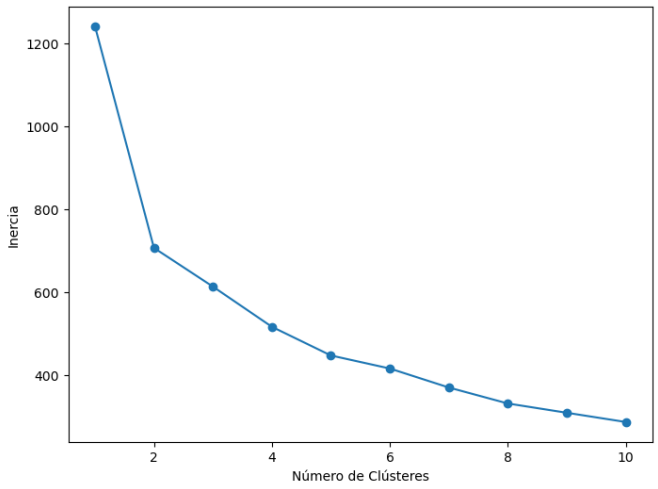


Figura 46 Método del Codo para Obtener Numero de Clusteres
Fuente: Elaboración Propia.

Para determinar la cantidad óptima de clústeres en el modelo K-Means, se utilizó el método del codo, el cual evalúa la inercia o suma de las distancias al centroide dentro de cada clúster. El análisis del gráfico resultante mostró un cambio significativo en la pendiente entre los valores 4 y 5, lo que indica que este rango es el más adecuado para segmentar los datos de manera eficiente.

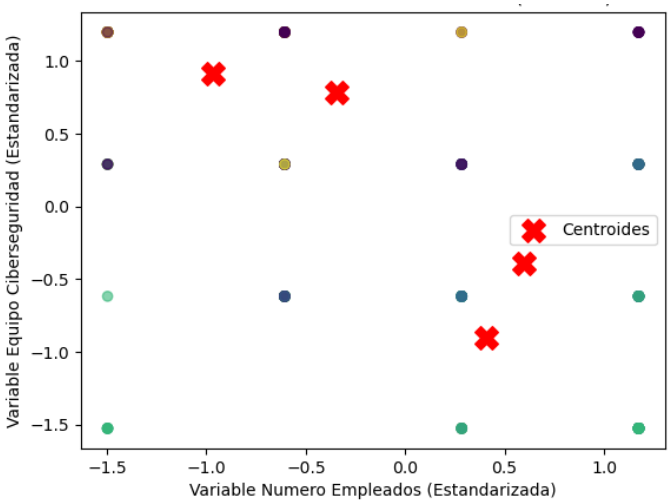


Figura 47 Clustering por K-Means
Fuente: Elaboración Propia.

Este gráfico de clustering, generado por K-Means, segmenta empresas según su número de empleados y la calidad de su equipo de ciberseguridad, revelando grupos de riesgo diferenciados para ataques de ransomware: el clúster inferior izquierdo, con empresas de pocos empleados y seguridad deficiente, representa el mayor riesgo, mientras que el clúster superior derecho, con empresas grandes y equipos sólidos, muestra el menor riesgo relativo, permitiendo así identificar patrones de vulnerabilidad y adaptar estrategias de prevención específicas..

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

1. Los resultados de la investigación han permitido identificar las principales vulnerabilidades y factores de riesgo que enfrentan las empresas hondureñas ante los ataques de ransomware. Se evidenció que un 52% de las empresas considera que existe muy poca conciencia sobre esta amenaza, lo que indica que el desconocimiento de los riesgos es una de las barreras más significativas para mejorar la ciberseguridad. Asimismo, la falta de presupuesto y la escasez de personal especializado limitan la capacidad de las empresas para implementar medidas de protección adecuadas. Un dato preocupante es que 97 empresas (49%) no cuentan con un plan de contingencia documentado, lo que las deja altamente vulnerables ante incidentes de ransomware, también se identificó que 40 empresas (19%) indicaron que no cuentan con medidas de seguridad específicas, lo que refleja una falta de preparación generalizada.

   La ausencia de políticas claras, junto con la falta de apoyo de la alta dirección y la baja frecuencia de actualización de políticas de seguridad, incrementa el riesgo de sufrir ataques exitosos. A esto se suma el factor humano, que sigue siendo un eslabón débil en la ciberseguridad, la combinación de baja concienciación, escasez de personal especializado, falta de inversión y ausencia de planes de contingencia crea un entorno altamente riesgoso para las empresas en Honduras. Estas vulnerabilidades están estrechamente relacionadas, pues sin conciencia sobre el problema, no hay presión para contratar expertos o asignar presupuesto a la seguridad digital. Esto evidencia la urgencia de desarrollar estrategias de protección y respuesta adaptadas al contexto hondureño, promoviendo una mayor educación en ciberseguridad, inversión en infraestructura tecnológica y adopción de normativas obligatorias.

2. Los datos recopilados confirman la necesidad de un plan de contingencia estructurado que contemple medidas preventivas, de detección, respuesta y recuperación. Actualmente, solo 37 empresas han probado su plan de contingencia mediante simulacros, lo que indica que la gran mayoría no ha evaluado su efectividad ante un ataque real, lo que evidencia la importancia de contar con protocolos bien definidos para mitigar el impacto del ransomware y otra tendencia relevante es la dependencia de las copias de seguridad como

principal estrategia de recuperación, ya que 80 empresas realizan respaldos diarios, pero 54 no cuentan con sistemas de respaldo, lo que las deja expuestas a la pérdida total de su información. Además, un 51% de las empresas no tiene un plan de acción definido en caso de un ataque, lo que indica la falta de preparación ante este tipo de incidentes.

Para abordar esta problemática, es indispensable que las empresas hondureñas adopten normativas reconocidas como NIST combinado con las ISO 22301 e ISO 27001, las cuales establecen marcos de referencia para la gestión de continuidad del negocio y seguridad de la información y el implementar un enfoque basado en prevención, detección, respuesta y recuperación. La adopción de estos elementos fortalecerá la postura de seguridad de las empresas hondureñas y permitirá minimizar el impacto de los ataques de ransomware. Sin embargo, más allá de la implementación de herramientas y procesos, es fundamental que las organizaciones comprendan la importancia de la ciberseguridad como un pilar estratégico para la continuidad del negocio. Sin un cambio de mentalidad hacia la seguridad proactiva, la vulnerabilidad ante ataques seguirá siendo un problema crítico en el país.

5.2 RECOMENDACIONES

1. Ante la evidente falta de preparación, es fundamental incrementar la capacitación en ciberseguridad, ya que 146 empresas identificaron la formación obligatoria de empleados como la estrategia más efectiva para fortalecer la seguridad. Se recomienda la implementación de programas educativos permanentes que aborden temas como reconocimiento de ataques de phishing, uso de autenticación multifactor y buenas prácticas en el manejo de datos sensibles. También es crucial fomentar la realización de simulacros de ciberataques, ya que solo una minoría de las empresas ha probado su plan de contingencia.

   Además, es fundamental que el gobierno hondureño y los organismos reguladores establezcan políticas obligatorias de ciberseguridad, exigiendo que empresas públicas y privadas cumplan con estándares internacionales como ISO 27001, ISO 22301 y el NIST Cybersecurity Framework. Esto garantizaría que la ciberseguridad sea tratada como un pilar estratégico dentro de las organizaciones y no solo como una medida reactiva ante incidentes. Con esta estrategia integral, las empresas hondureñas podrán fortalecer su postura de seguridad, minimizar el riesgo de incidentes y generar una cultura

organizacional orientada a la protección de la información.

2. Para garantizar la implementación efectiva de un plan de contingencia ante ataques de ransomware, se recomienda estructurarlo en cuatro fases clave: **prevención, detección, respuesta y recuperación**, asegurando que cada una cuente con protocolos específicos y pruebas periódicas que validen su efectividad, donde la **Prevención** (Reducción del Riesgo de Ataques), las organizaciones deban adoptar estrategias proactivas que disminuyan su vulnerabilidad frente al ransomware. Según los datos recopilados, la falta de actualización de software y la escasa capacitación del personal han sido factores críticos en ataques previos. Para mitigar estos riesgos, también en la fase **Detección** (Identificación Temprana de Amenazas), es fundamental implementar sistemas avanzados de monitoreo que permitan identificar y responder rápidamente a posibles amenazas. Según el análisis de datos, muchas empresas hondureñas carecen de herramientas avanzadas para la detección temprana de ataques.

   La **Respuesta** (Contención y Mitigación del Ataque), La rapidez con la que se actúe en esta fase determinará el impacto del ransomware en la empresa. Actualmente, el 51% de las empresas encuestadas no tiene un plan de acción definido, lo que aumenta la posibilidad de una respuesta ineficaz, Finalmente, **la Recuperación (**Restauración y Mejora Continua**),** esta debe centrarse en la restauración segura de los datos, evaluación post-incidente y mejoras en las políticas de seguridad. Además, para fortalecer la capacidad de respuesta a nivel nacional, se sugiere la creación de un Centro Nacional de Respuesta a Incidentes (CSIRT Nacional), estrategia que 64 empresas identificaron como clave para la mejora de la ciberseguridad en Honduras. Este centro permitiría una respuesta coordinada entre empresas y entidades gubernamentales, facilitando la gestión centralizada de incidentes y la difusión de alertas tempranas sobre nuevas amenazas.

CAPÍTULO VI. APLICABILIDAD

6.1 NOMBRE DE LA PROPUESTA

Plan de Contingencia y Respuesta ante Ciberataques de Tipo Ransomware para Empresas en Honduras

6.2 JUSTIFICACIÓN DE LA PROPUESTA

La creciente amenaza del ransomware se ha convertido en una de las principales preocupaciones en el ámbito de la ciberseguridad empresarial, comprometiendo la continuidad operativa, la integridad de los datos y la estabilidad financiera de las organizaciones. En Honduras, muchas empresas carecen de protocolos adecuados para prevenir, detectar, responder y recuperarse de estos ataques, lo que incrementa su vulnerabilidad y las expone a pérdidas significativas.

Esta propuesta tiene como objetivo fortalecer la ciberseguridad empresarial a través de la implementación de un marco estratégico basado en normativas internacionales, incluyendo la **ISO 22301** (Gestión de la Continuidad del Negocio), para garantizar que las empresas cuenten con planes de contingencia estructurados que les permitan continuar operando tras un ataque de ransomware como la **ISO 27001** (Seguridad de la Información), usada para establecer un sistema de gestión de seguridad que refuerce la protección de los datos y minimice el riesgo de incidentes cibernéticos, asimismo la **NIST Cybersecurity Framework,** para proporcionar un enfoque integral y adaptable basado en cinco funciones clave: **Identificar, Proteger, Detectar, Responder y Recuperar**, lo que permite a las empresas evaluar continuamente su postura de seguridad y optimizar sus estrategias de defensa.

La aplicación de este marco estratégico permitirá que las empresas hondureñas:

- Reduzcan su exposición al ransomware mediante controles preventivos efectivos.
- Detecten ataques en tiempo real con herramientas avanzadas de monitoreo.
- Respondan rápidamente a incidentes mediante protocolos bien definidos.
- Se recuperen de forma segura y eficiente, minimizando el impacto financiero y operativo.

Además, la adopción de estos estándares fortalecerá la confianza de clientes y socios comerciales, al demostrar que la empresa cuenta con medidas sólidas y alineadas con las mejores

prácticas internacionales. Con este enfoque, se busca transformar la ciberseguridad en Honduras, pasando de un modelo reactivo a uno proactivo y resiliente, garantizando así un entorno empresarial más seguro y preparado para enfrentar los desafíos del ransomware y otras amenazas emergentes.

6.3 ALCANCE DE LA PROPUESTA

El Plan de Contingencia y Respuesta ante Ransomware está dirigido a empresas hondureñas de distintos sectores, en especial aquellas que **Manejan información crítica**, como entidades financieras, empresas de telecomunicaciones, hospitales, aseguradoras y organismos gubernamentales, que **Dependen de la disponibilidad continua de sus sistemas**, como el comercio electrónico, servicios en la nube y empresas industriales con sistemas automatizados y los que **Cuentan con recursos limitados para la ciberseguridad**, como PYMEs que aún no han implementado medidas de protección avanzadas.

Este plan busca proporcionar una **estrategia estructurada y adaptable** que permita mejorar la **resiliencia empresarial** frente a ataques de ransomware, independientemente del tamaño o sector de la empresa.

El plan se desarrollará en cuatro fases principales, las cuales pueden ejecutarse de manera independiente o combinada, dependiendo del nivel de madurez de seguridad de cada empresa:

1. **Prevención**: Establecimiento de controles de seguridad y capacitación del personal.
2. **Detección**: Implementación de herramientas de monitoreo y análisis de amenazas.
3. **Respuesta:** Definición de protocolos de actuación ante un ataque de ransomware.
4. **Recuperación**: Estrategias para restauración de datos y evaluación post-incidente.

El modelo propuesto es escalable y adaptable, permitiendo su aplicación tanto en pequeñas empresas como en grandes corporaciones.

Limitaciones y Desafíos en el Contexto Hondureño

A pesar de su flexibilidad y aplicabilidad, la implementación de este plan enfrenta algunos desafíos y limitaciones, entre ellos:

- Baja cultura de ciberseguridad: Muchas empresas aún no consideran la ciberseguridad una prioridad, lo que dificulta la adopción de medidas preventivas.

- Limitaciones presupuestarias: Especialmente en PYMEs, donde la inversión en herramientas avanzadas y personal especializado puede ser restringida.
- Escasez de talento especializado: Existe una falta de profesionales capacitados en ciberseguridad, lo que complica la implementación y mantenimiento del plan.
- Falta de regulaciones estrictas: En Honduras, la ciberseguridad aún no está completamente regulada, lo que impide la obligatoriedad de medidas de protección en todos los sectores.

6.4 DESCRIPCIÓN Y DESARROLLO

6.4.1 DESCRIPCIÓN

La propuesta consiste en el diseño de un Plan de Contingencia y Respuesta ante Ransomware para mejorar la ciberseguridad y continuidad operativa en las empresas hondureñas. Este plan se basa en buenas prácticas internacionales y busca proporcionar un enfoque preventivo y reactivo ante ataques cibernéticos, donde el plan estará desarrollado basado en las normativas de estandarización ISO 27001 en la que se aplicarán algunas de sus fases junto con el modelo PHVA de Deming y la ISO 22301 que es la norma para poder mantener la continuidad del negocio.

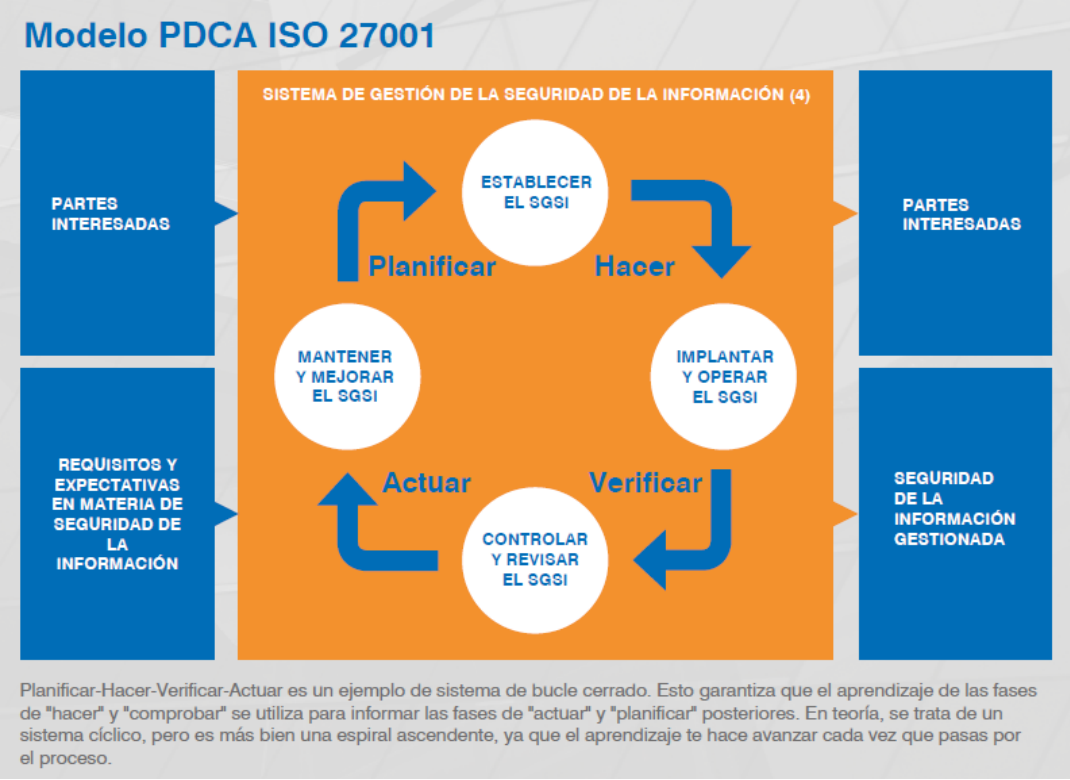


Figura 48 Ciclo PHVA enfocado en la ISO 27001
Fuente: ISO 27001:2022 IMPLEMENTATION GUIDE.

Ransomware

El ransomware es un tipo de malware que cifra los archivos o sistemas de una víctima, impidiéndole el acceso a su propia información. Los atacantes exigen un pago, generalmente en criptomonedas, a cambio de la clave de descifrado que permitiría recuperar los datos. Este tipo de ataque puede afectar tanto a individuos como a empresas y gobiernos, causando pérdidas económicas, interrupciones operativas y daños reputacionales.

La única manera de desencriptar los archivos bloqueados por el ransomware es mediante una clave de desencriptado que está en poder de los atacantes. Cada vez es más común que las bandas de ransomware roben también los datos de una organización para tener más ventaja durante las negociaciones del rescate.

Figura 49 Ransomware
Fuente: ministerio de ciencia, innovación, tecnología y telecomunicaciones, Costa rica.

6.4.2 DESARROLLO

La mayoría de las empresas tienen información valiosa o confidencial que proteger adecuadamente, el no hacerlo puede tener serias consecuencias de acción, financiera y legal. En algunos casos, pueden hacer que la compañía tenga una quiebra total al tener un ataque de tipo ransomware. El desafío que enfrenta la mayoría de las empresas es cómo ofrecer protección suficiente. Específicamente, ¿cómo se aseguran de haber identificado todos los riesgos a los que están expuestos y cómo pueden controlarlos de una manera proporcional, sostenible y efectiva? El

modelo por proponer es una combinación entre el estándar reconocido internacionalmente para el Sistema de Gestión de Seguridad de la Información (SGSI) y ciertas medidas que nos permitirán la continuidad del negocio, siempre manteniendo la calma ante un evento de ataque.

Proporcionando un sistema estable para proteger la información que se puede personalizar a todo tipo y tamaño de organizaciones. Las organizaciones que están muy sujetas a la seguridad de la información se eligen cada vez más para introducir SGSI, que corresponde a ISO 27001, para ello se establecen 4 fases de trabajo para este plan de contingencia y respuesta eficaz para ataques tipo Ransomware y antes de esas fases, debemos tener un espacio de preparación que se estructura de la siguiente manera.

Preparación

La preparación es un componente importante para la construcción de capacidades efectivas de respuesta a incidentes. Esta sección facilita una descripción general de los procesos implementados para ayudar a mitigar el riesgo de ransomware y las funciones, como también responsabilidades de las partes interesadas clave.

Se recomienda que las secciones descritas en esta fase sean personalizadas para adaptarse a la empresa a implementar, ya que por capacidades o circunstancias diferentes pueden cambiar de una a otra, a continuación, se desglosan cada una de las secciones expuestas para que la preparación sea efectiva:

- **Funciones y responsabilidades**:

  Defina claramente las partes interesadas clave, proporciona funciones y responsabilidades actualizadas y describa las necesidades acciones si se detecta un ataque de ransomware.

- **Capacitación en concientización sobre seguridad:**

  Implementar la capacitación en seguridad requerida en toda la empresa para comunicar los peligros de las amenazas maliciosas y orientación para identificar actividades sospechosas con medidas para proteger. Educar a los usuarios sobre cómo informar actividad cuestionable a los equipos de seguridad.

- **Copias de seguridad y recuperación de datos**

  Se debe realizar una copia de seguridad de todos los datos y metadatos importantes

periódicamente en una bóveda que sea inmutable, con espacios de aire y enjaulados. Se recomiendan simulacros parciales para asegurarse de que los datos sean válidos y recuperables.

- **Configuración de herramientas de seguridad**
    - Procure instalar firewall de red y de aplicaciones -WAF, sistema Endpoint Detection Response EDR, para obtener visibilidad en la red.
    - Asegúrese de que existan programas, políticas y procedimientos para administrar terminales y dispositivos móviles para que los dispositivos sean más resistentes al ransomware y otras infecciones de malware. Ejemplos: endurecer requisitos, instalar soluciones antivirus y antimalware, actualizar sistemas operativos y aplicaciones, etc.
    - Invierta en soluciones basadas en XDR como Microsoft Defender para Endpoint para proteger sus dispositivos.
- **Protección de red**

  Garantizar que se implementen programas, políticas y procedimientos para monitorear y asegurar la entrada y salida. apunta a la red: firewalls, uso de acceso con privilegios mínimos, aplicación de autenticación sólida, métodos como la autenticación multifactor (MFA), soluciones antispam para correo electrónico, etc. Invierta en un software basado en SIEM como Microsoft Sentinel para acceder a funciones avanzadas de información valiosa con análisis de comportamiento integrados para adelantarse a los atacantes.
- **Uso de VPN**

  La configuración de una VPN establece un túnel cifrado de comunicación entre el equipo que sale a internet e Internet, estableciendo una conexión segura, garantizando protección frente a amenazas externas.
- **Desactivación de unidades externas**

  Desactive las opciones Autorun y Autoplay en las unidades externas (CD, USB, etc.), de igual forma minimice el uso de conexión de dispositivos externos por parte de los colabores en los computadores de la organización.

- **Configuración de correo corporativo con filtros antispam**

  El filtro antispam mantiene la bandeja de entrada libre de spam y phishing, se puede realizar a correos comerciales.

- **Plan de auditoría de logs del sistema**

  Implemente plan de auditoría de logs permanente, de las actividades de gestión del Directorio Activo, como cambios de contraseñas, eliminación de usuario, creación y/o modificación de cuentas de usuario, etc.

- **Programación de pruebas de vulnerabilidad**

  Las pruebas de vulnerabilidades aplicadas regularmente permiten revisar y estimar las debilidades de seguridad en la infraestructura de un sistema de información.

- **Limitar el uso de escritorio remoto (RDP)**

  Los actores de amenazas generalmente acceden una red a través de servicios remotos desprotegidos.

- **Políticas de seguridad**

  Las políticas de seguridad deben mantenerse actualizadas y aplicarse para todas las identidades, usuarios y cuentas que tienen acceso a los activos y recursos de la empresa.

- **Plan de continuidad**

  El desarrollo de un plan de continuidad, para definir las aplicaciones de misión crítica que deben ser respaldadas en sitio alterno para la recuperación y restablecimiento de las operaciones según el tiempo tolerable necesario para que los sistemas críticos vuelvan a estar operativos (RTO) y la cantidad máxima aceptable de pérdida de datos entre la última copia de seguridad y la fecha en que ocurre del incidente (RPO).

- **Principio del mínimo privilegio – Zero Trust**

  Administre y supervise las cuentas de usuario y el acceso aplicando el principio de mínimos privilegios.

- **Deshabilitar macros**

Asegúrese de deshabilitar las macros como predeterminadas, para reducir el riesgo que el ransomware se propague a través de los archivos adjuntos de Microsoft Office.

También podemos analizar que tenemos o que nos hace falta en la parte de preparación con ayuda de la siguiente tabla cabe destacar que siempre es conveniente identificar los riesgos a los que estamos expuestos:

Tabla 13 Lista de comprobación para la protección proactiva

Lista de comprobación para la protección proactiva contra el ransomware.	Intrusión	Infiltración	Ataque	Restablecimiento	Recuperación
Crear un inventario de activos, incluyendo hardware, software y datos.	X	X			
Auditar la red en busca de computadoras y servicios desconocidos.	X	X			
Desactivar los sistemas, servicios y puertos de Internet que no son necesarios.	X	X			
Realizar escaneos regulares de vulnerabilidad.	X	X			
Parchar los sistemas regularmente, dando prioridad a los más vulnerables y críticos.	X	X			
Garantizar que los sistemas están correctamente configurados y que las funciones de seguridad están activadas.	X	X			
Reforzar la seguridad del acceso remoto con autenticación de factores múltiples (MFA), límites de tasa de las contraseñas y bloqueos de contraseñas.	X				
Implementar software de seguridad para puntos finales en todos los puntos y **servidores.**	X	X	X		
Proporcionar al personal capacitación en materia de ciberseguridad.	X	X			
Implementar un proceso para informar y responder a actividades sospechosas.	X	X	X		
Documentar la estructura de la red y los lujos de datos.		X			X
Utilizar la segmentación de la red para subdividir las redes informáticas.		X			
Utilizar el acceso de mínimo privilegio para todos los sistemas y servicios	X	X			
Utilizar la lista de permisos para garantizar que solo se pueda ejecutar el software autorizado		X	X		
Restringir el uso de herramientas legítimas utilizadas habitualmente por los atacantes		X			
Reforzar la protección de los controladores de dominio de acuerdo con las mejores prácticas más recientes.		X			
Supervisar la red y sus puntos finales mediante sistemas de detección de intrusiones (IDS), detección y respuesta de punto final (EDR) y sistemas de gestión de eventos e información de seguridad (SIEM).		X	X		X

Lista de comprobación para la protección proactiva contra el ransomware.	Intrusión	Infiltración	Ataque	Restablecimiento	Recuperación
Realizar copias de seguridad continuas y completas y asegurarse de que por lo menos una de ellas no esté conectada a la red.				X	
Disponer de un proceso de restablecimiento de computadoras a partir de imágenes limpias del sistema				X	
Practicar el restablecimiento de sistemas a partir de copias de seguridad, para asegurarse de que funcionan.				X	
Crear un plan de respuesta a incidentes que se ajuste a la normativa			X	X	
Crear una lista de activos críticos para saber qué se debe restaurar primero.				X	

Fuente: Elaboración propia

Una vez visualizada la preparación, las prácticas recomendadas y las referencias que se indican en esta sección son para ayudar a administrar los riesgos que plantea el ransomware e impulsar una respuesta coordinada y eficiente para su organización en caso de un incidente. Aplique estos procesos que a continuación se muestra, en la mayor medida posible según la disponibilidad de recursos organizacionales.

6.4.2.1 PREVENCIÓN

Objetivo

Establecer estrategias y controles de seguridad proactivos que reduzcan la probabilidad de un ataque de ransomware, protegiendo la infraestructura tecnológica, los datos y los usuarios de la organización.

Alcance

El proceso abarca todas las infraestructuras tecnológicas, sistemas de información, redes y usuarios dentro de la organización que puedan ser vulnerables a un ataque de ransomware.

Responsables

- Equipo de seguridad informática
- Administrador de sistemas y redes
- Director de TI

- Alta dirección
- Usuarios finales

Terminología

Segmentación de Red: Estrategia de seguridad que divide la red en segmentos aislados para limitar la propagación de malware y restringir el movimiento lateral de atacantes en caso de una intrusión.

Principio de Mínimo Privilegio (PoLP): Enfoque de seguridad que garantiza que cada usuario, cuenta o sistema solo tenga acceso a los recursos esenciales para su función, reduciendo el riesgo de explotación en caso de compromiso.

Cifrado de Datos Sensibles: Implementación de técnicas criptográficas para proteger información crítica contra accesos no autorizados, asegurando su confidencialidad tanto en tránsito como en reposo.

Conciencia en Ciberseguridad: Programa educativo dirigido a empleados y usuarios finales con el objetivo de fortalecer la cultura de seguridad, promoviendo buenas prácticas y reduciendo riesgos asociados a ataques de ingeniería social.

Actividades

1. **Implementar controles de acceso y segmentación de red:** Definir políticas de acceso basadas en roles y restringir conexiones entre sistemas críticos para minimizar la exposición a ataques.
2. **Mantener actualizados los sistemas y aplicar parches de seguridad**: Establecer un plan de actualización regular para disminuir el riesgo ante ataques de ransomware.
3. **Configurar respaldos de seguridad periódicos**: Implementar copias de seguridad automáticas y almacenarlas en ubicaciones protegidas y fuera de línea.
4. **Capacitar al personal en identificación de amenazas**: Realizar campañas de conciencia sobre phishing, ransomware y buenas prácticas de seguridad.
5. **Simulación de ataques**: Realizar ejercicios de seguridad y simulaciones de ataques para evaluar la efectividad de los controles preventivos.

Diagrama de flujo

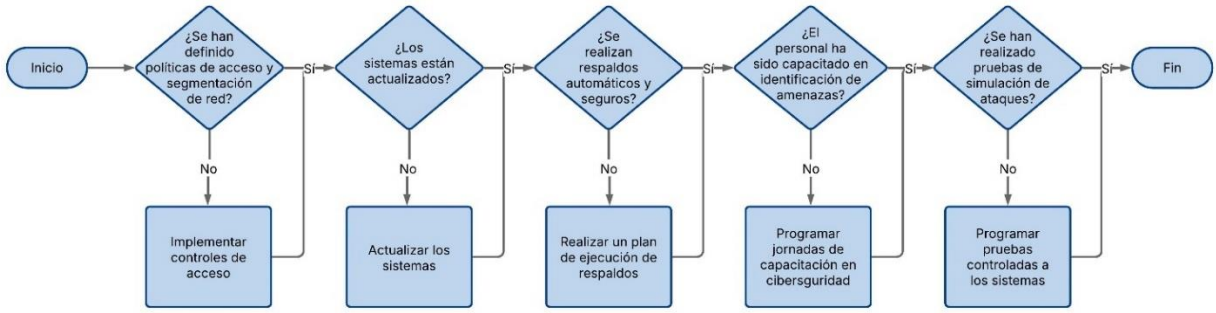


Figura 50 Diagrama de Flujo de Prevención
Fuente: Elaboración propia.

6.4.2.2 DETECCIÓN

Objetivo

Establecer mecanismos y estrategias para la identificación temprana de intentos de ataque de ransomware, permitiendo una respuesta rápida para minimizar su impacto en la organización.

Alcance

El proceso de detección abarca todas las infraestructuras tecnológicas, redes, sistemas de información y actividades de los usuarios dentro de la organización que puedan ser objeto de un ataque de ransomware.

Responsables

- Equipo de seguridad informática
- Administrador de sistemas y redes
- Director TI

Terminología

Monitoreo de Eventos de Seguridad: Sistema que centraliza la recopilación, análisis y correlación de eventos de seguridad en tiempo real para detectar actividades sospechosas o anómalas en la red y los sistemas.

Indicadores de Compromiso: Evidencias detectables de que un sistema ha sido comprometido por ransomware, incluyendo tráfico anómalo, cambios inesperados en archivos y

ejecución de procesos desconocidos.

Análisis de Comportamiento de Usuarios y Dispositivos: Técnica de detección basada en la identificación de patrones de comportamiento anómalos en usuarios y dispositivos, permitiendo reconocer accesos sospechosos o actividad maliciosa.

Actividades

1. **Implementar sistemas de monitoreo y análisis de seguridad**: Configurar herramientas como SIEM y UEBA para detectar comportamientos anómalos en la red y los sistemas.
2. **Analizar registros y eventos en busca de indicadores de compromiso:** Revisar continuamente logs de actividad para identificar posibles señales de un ataque en curso.
3. **Detectar tráfico sospechoso:** Utilizar firewalls y sistemas de detección de intrusos (IDS/IPS) para identificar conexiones maliciosas o transferencias de datos no autorizadas. También se puede utilizar software de captura de paquetes como Wireshark.
4. **Activar alertas tempranas ante cambios anómalos en archivos o sistemas:** Configurar herramientas de monitoreo que detecten modificaciones inesperadas en archivos, picos en el uso del CPU o actividad inusual en cuentas de usuario.
5. **Fomentar la notificación de actividades sospechosas por parte de los usuarios:** Sensibilizar a los empleados para que reporten comportamientos anómalos, correos electrónicos sospechosos o fallos inusuales en los sistemas.

Diagrama de flujo

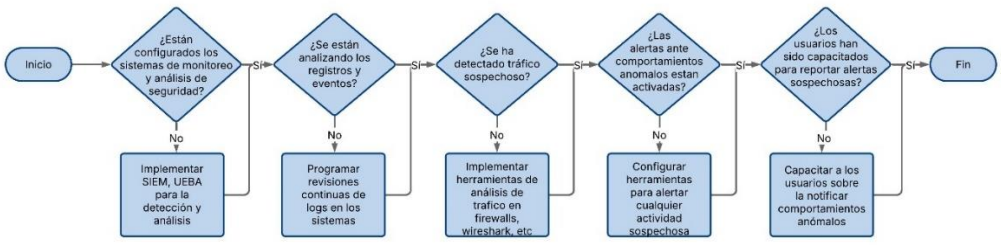


Figura 51 Diagrama de Flujo de Detección
Fuente: Elaboración propia.

6.4.2.3 RESPUESTA

Objetivo

Establecer un protocolo de respuesta inmediata para contener la propagación del ransomware, minimizando el impacto en los sistemas afectados y evitando que los dispositivos dentro de la red empresarial sean afectados.

Alcance

El alcance del proceso comprende a todas las infraestructuras tecnológicas, datos, sistemas y usuarios dentro de la organización que puedan ser afectados por un ransomware.

Responsables

- Equipo de Seguridad Informática
- Administrador de Sistemas y Redes
- Director de TI
- Alta Dirección

Terminología

Aislamiento de Sistemas: Proceso de desconectar o segmentar los dispositivos y redes afectadas para evitar la propagación del ransomware y minimizar el impacto del ataque en la infraestructura de TI. Puede incluir la desconexión física o lógica de sistemas críticos.

Notificación del Incidente: Comunicación formal del ataque de ransomware a las partes interesadas, incluyendo el equipo de TI, alta dirección, empleados, clientes y, si aplica, autoridades regulatorias. Su objetivo es coordinar una respuesta efectiva y mitigar daños adicionales.

Evaluación del Daño: Análisis detallado del impacto del ataque en términos de datos cifrados, pérdida de información, interrupción de operaciones y posibles filtraciones de datos. Esta evaluación permite priorizar la recuperación y definir las acciones correctivas necesarias.

Análisis Forense Digital: Proceso de investigación técnica del ataque para identificar la variante del ransomware, determinar el punto de acceso inicial, rastrear la actividad del atacante y recopilar evidencia útil para mejorar la seguridad y prevenir futuros incidentes.

Actividades

1. **Determinar sistemas afectados y aislarlos de inmediato:** Priorizar aislamiento de sistemas fundamentales que son necesarios para la continuidad del negocio.
2. **Apagar dispositivos en caso de no poder desconectarlos de la red para evitar una mayor propagación**: Esta acción debe llevarse a cabo en caso no ser posible apagar temporalmente la red o desconectar los hosts afectados de la red.
3. **Evaluar el alcance del ataque**: Realizar una evaluación inicial del alcance y gravedad del ataque, involucrando a todas las partes interesadas. También será necesario realizar un inventario de los activos comprometidos.
4. **Clasificar los sistemas afectados para la restauración y recuperación:** Identificar y priorizar sistemas fundamentales para una posterior restauración en una red limpia.
5. **Comunicar el incidente:** Es clave informar sobre el incidente a las partes interesadas, empleados, clientes, socios, sobre el ataque y las medidas que se están ejecutando.
6. **Registro y documentación del incidente**: Registrar las acciones ejecutadas, sistemas afectados y los hallazgos técnicos. Documentar evidencia para facilitar la investigación.
7. **Coordinación con expertos y autoridades**: Determinar si es necesario contactar equipos forenses, proveedores de ciberseguridad o autoridades reguladoras relacionadas a este tipo de incidentes.

Diagrama de Flujo

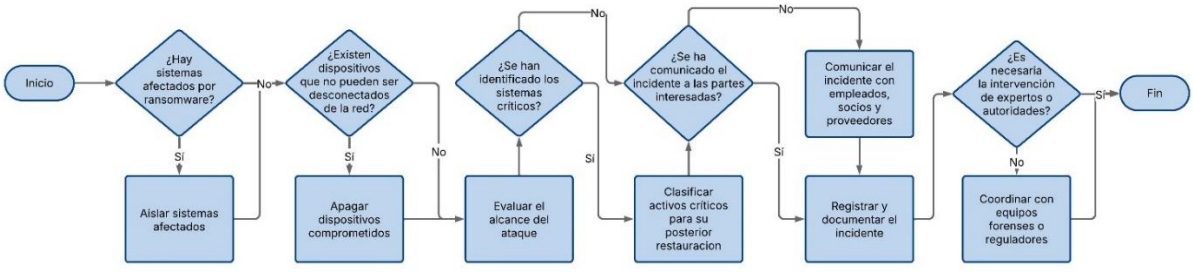


Figura 52 Diagrama de Flujo de Respuesta
Fuente: Elaboración propia.

6.4.2.4 RECUPERACIÓN

Objetivo

Restaurar los sistemas y datos afectados por un ataque de ransomware de manera segura y eficiente, minimizando el tiempo de inactividad y asegura la continuidad de las operaciones de la organización.

Alcance

El alcance de este proceso comprende toda aquella infraestructura tecnológica, dispositivos, información y usuarios afectados por un ataque de ransomware.

Responsables

- Equipo de seguridad informática
- Gerente de TI
- Administrador de sistemas y redes
- Alta dirección

Terminología

Restauración de Sistemas: Proceso de recuperación de servidores, dispositivos y aplicaciones afectadas por el ransomware utilizando copias de seguridad o configuraciones previas al ataque.

Integridad de Datos: Verificación de que los datos restaurados no han sido alterados o comprometidos por el ransomware y que pueden ser utilizados de manera segura.

Actividades

1. **Restaurar sistemas afectados**: Reconectar sistemas afectados y restaurar las copias de seguridad de aquellos activos priorizados anteriormente en el proceso de respuesta.
2. **Documentar lecciones aprendidas**: Documentar cada una de las acciones ejecutadas durante todo el incidente. Evaluar si el proceso de respuesta ante el ataque fue el más adecuado y optimo.
3. **Realizar las mejoras de seguridad correspondientes**: Después de contener el

ataque y restaurar los sistemas, se tiene que realizar una revisión exhaustiva de sus medidas de seguridad

Diagrama de Flujo

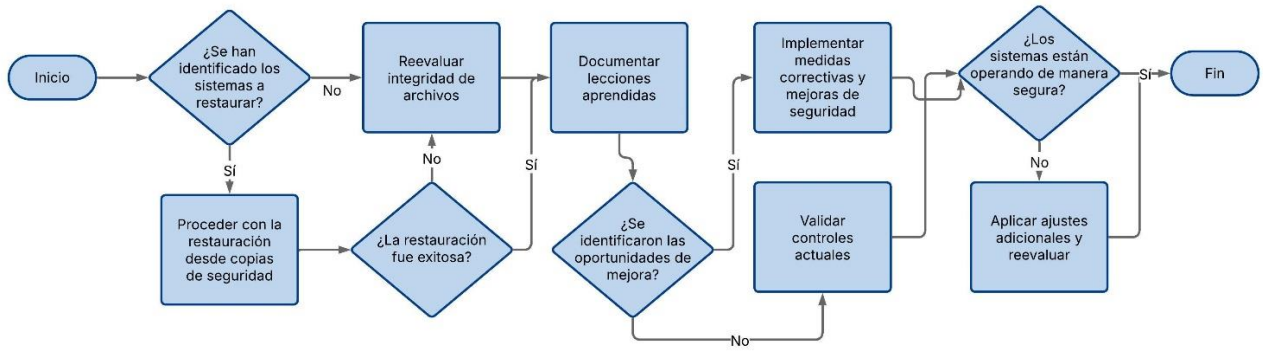


Figura 53 Diagrama de Flujo de Recuperación
Fuente: Elaboración propia.

Replicabilidad en Otros Contextos

El enfoque modular del plan permite su aplicación en diferentes sectores y tamaños de empresas. Para garantizar su replicabilidad, se han identificado factores clave de adaptación según el tipo de organización:

Tabla 14 Replicabilidad en otros contextos

Tipo de Empresa	Consideraciones Claves para la Adaptación
Pequeñas Empresas (PYMEs)	• Implementación gradual según disponibilidad de recursos. • Priorización de medidas esenciales como copias de seguridad y MFA. • Capacitación básica para empleados con acceso a información crítica.
Empresas de Mediano Tamaño	• Integración de herramientas avanzadas de monitoreo y respuesta a incidentes. • Pruebas de recuperación y simulacros anuales. • Creación de un equipo responsable de la ciberseguridad interna.
Grandes Corporaciones	• Implementación de SIEM y sistemas de detección de amenazas en tiempo real. • Plan de comunicación y respuesta ante crisis alineado con ISO 22301. • Simulacros regulares para evaluar la efectividad del plan.
Entidades Gubernamentales y Financieras	• Cumplimiento con regulaciones específicas y normativas internacionales. • Integración con Centros Nacionales de Respuesta a Incidentes (CSIRT). • Desarrollo de políticas de respuesta ante ataques dirigidos y APTs.

Fuente: Elaboración propia

6.5 MEDIDAS DE CONTROL

Para garantizar la efectividad del Plan de Contingencia y Respuesta ante Ransomware en las empresas hondureñas, se han definido medidas de control estructuradas en cada una de sus fases: **prevención, detección, respuesta y recuperación**. En la fase de prevención, se aplican estrategias como la segmentación de red y autenticación multifactor (MFA) para restringir accesos no autorizados, además de actualizaciones de seguridad periódicas y capacitaciones en concienciación sobre ciberseguridad, incluyendo simulaciones de ataques de phishing. En la fase de detección, se emplean herramientas de monitoreo como SIEM, IDS/IPS y análisis de comportamiento para identificar anomalías, mientras que el personal es capacitado para reconocer y reportar actividades sospechosas.

Durante la fase de respuesta, se activa el CSIRT (Equipo de Respuesta ante Incidentes), ejecutando protocolos de aislamiento de sistemas comprometidos, evaluación del impacto del ataque y coordinación con autoridades y expertos en ciberseguridad. Finalmente, en la fase de recuperación, se garantiza la restauración segura de sistemas desde copias de seguridad inmutables, análisis forense post-ataque y actualización de medidas de seguridad para fortalecer la resiliencia empresarial.

6.5.1 INDICADORES

Tabla 15 Indicadores claves de desempeño

Categoría	KPI	Tipo	Meta / Umbral	Frecuencia	Responsable	Observaciones
Capacitación	% de empleados capacitados en ciberseguridad	Cuantitativo	≥ 90% de los empleados entrenados	Cada 3 meses	Departamento de RRHH	Medir el impacto de la capacitación en la reducción de incidentes.
Simulacros	N.º de simulaciones de phishing realizadas	Cuantitativo	≥ 4 simulaciones al año	Anual	Equipo de Ciberseguridad	Evaluar la efectividad de los simulacros y ajustar las medidas de seguridad.
Seguridad Técnica	Nivel de cumplimiento de actualizaciones de seguridad	Cuantitativo	≥ 95% de los sistemas actualizados	Mensual	Equipo de TI	Identificar sistemas que requieren atención urgente.
Detección	Tiempo promedio de detección de un incidente	Cuantitativo	≤ 15 minutos	Mensual	Equipo de Ciberseguridad	Analizar las causas de demoras y mejorar los procesos de

Categoría	KPI	Tipo	Meta / Umbral	Frecuencia	Responsable	Observaciones
						detección.
Alertas	N.º de alertas de seguridad analizadas	Cuantitativo	≥ 95% de las alertas críticas revisadas	Mensual	Equipo de Ciberseguridad	Priorizar alertas críticas y mejorar la eficiencia del análisis.
Reportes	Eficiencia de reportes de usuarios ante intentos de phishing	Cualitativo	Evaluación post-simulacro	Cada 3 meses	Equipo de Ciberseguridad	Evaluar la efectividad de los simulacros y ajustar las medidas de seguridad.
Respuesta	Tiempo de respuesta ante un incidente	Cuantitativo	≤ 30 minutos desde la detección	Mensual	Equipo de Ciberseguridad	Analizar las causas de demoras y mejorar los procesos de respuesta.
Contención	% de incidentes contenidos exitosamente	Cuantitativo	≥ 85% de los casos	Anual	Equipo de Ciberseguridad	Identificar áreas de mejora en los procedimientos de contención.
Coordinación	Coordinación con organismos externos	Cualitativo	Evaluación post-incidente	Post-incidente	Equipo de Ciberseguridad	Evaluar la efectividad de la coordinación y establecer protocolos de comunicación.
Recuperación	Tiempo promedio de restauración de datos	Cuantitativo	≤ 4 horas	Post-incidente	Equipo de Ciberseguridad	Analizar las causas de demoras y mejorar los procesos de restauración.
Integridad	% de datos recuperados sin alteraciones	Cuantitativo	≥ 98%	Post-incidente	Equipo de Ciberseguridad	Verificar la integridad de los datos recuperados y ajustar los procesos de respaldo.
Mejora Continua	Evaluación post-incidente y actualización de controles	Cualitativo	Informe de lecciones aprendidas	Post-incidente	Equipo de Ciberseguridad	Identificar lecciones aprendidas y aplicar mejoras en los controles de seguridad.

Fuente: Elaboración propia

6.5.2 PLAN DE SEGUIMIENTO

Se establece un proceso de monitoreo y control estructurado en cada fase: prevención, detección, respuesta y recuperación. Este plan define herramientas, responsables, frecuencia de revisión y protocolos paso a paso.

Tabla 16 Seguimiento de Medidas de Control

Fase	Acción de Seguimiento	Herramientas/ Procedimientos	Responsable	Frecuencia
Prevención	Auditoría de cumplimiento de segmentación de red y MFA	Revisiones con herramientas de administración de acceso (IAM, Active Directory)	Equipo de Seguridad TI	Trimestral
	Evaluación de efectividad de capacitaciones en ciberseguridad	Pruebas de phishing, encuestas de concienciación	Departamento de TI y RRHH	Trimestral
	Revisión de cumplimiento de actualizaciones de seguridad	Escaneos de vulnerabilidades con Nessus, Qualys	Equipo de Infraestructura	Mensual
Detección	Monitoreo de eventos sospechosos y análisis de tráfico	SIEM (Splunk, QRadar), IDS/IPS (Snort, Suricata)	Centro de Operaciones SOC	24/7 - Tiempo real
	Evaluación de alertas de seguridad generadas y revisadas	Revisión de registros en SIEM y correlación de eventos	Analistas de Seguridad	Diario
	Simulacro de ataque para evaluar detección	Simulación con herramientas como Red Teaming	Equipo de Seguridad TI	Semestral
Respuesta	Prueba de tiempos de respuesta ante incidentes simulados	Simulación de incidentes con equipos de respuesta	CSIRT / SOC	Semestral
	Revisión de protocolos de contención de ransomware	Auditoría de ejecución de procedimientos de contención	CSIRT / Equipo de Seguridad	Mensual
	Evaluación de incidentes reales y análisis de efectividad	Post-mortem de incidentes y revisión de documentación	Líder de Seguridad	Post-incidente
Recuperación	Validación de copias de seguridad y restauración de prueba	Pruebas de recuperación desde copias inmutables	Equipo de Infraestructura	Mensual
	Análisis forense post-ataque y mejora de controles	Uso de herramientas como Autopsy, Volatility	Equipo de Respuesta a Incidentes	Post-incidente
	Evaluación de la actualización de medidas de seguridad tras incidentes	Informe de lecciones aprendidas y corrección de fallos	CSIRT / Gestión de Riesgos	Post-incidente

Fuente: Elaboración propia

6.6 CRONOGRAMA DE IMPLEMENTACIÓN Y PRESUPUESTO

La fase de prevención recibe la mayor inversión y tiempo de ejecución, ya que una estrategia proactiva puede reducir significativamente la probabilidad de un ataque exitoso y la detección y respuesta están diseñadas para minimizar el impacto y contener el ataque rápidamente mientras la recuperación se enfoca en restaurar los sistemas de manera segura y fortalecer la ciberseguridad para futuras amenazas.

6.6.1 CRONOGRAMA DE IMPLEMENTACIÓN

Este cronograma detalla un plan estructurado de **6 meses** con actividades clave para garantizar que las empresas hondureñas estén preparadas ante un ataque de ransomware.

Tabla 17 Cronograma de implementación

Fase	Actividad Clave	Descripción	Responsables	Duración Estimada
1 Prevención	Implementación de controles de acceso y segmentación de red	Configuración de restricciones de acceso y separación de entornos críticos.	Equipo de TI / Seguridad Informática	Semana 1-2
	Actualización y aplicación de parches de seguridad	Establecer un proceso de actualización continua para evitar vulnerabilidades.	Administrador de Sistemas y Redes	Semana 3-4
	Configuración de respaldos de seguridad periódicos	Implementación de copias de seguridad automáticas, fuera de línea y cifradas.	Equipo de Seguridad / TI	Semana 4-5
	Capacitación en identificación de amenazas	Formación sobre ransomware, phishing y protocolos de seguridad.	RRHH / Seguridad Informática	Semana 6-7
	Simulación de ataques	Evaluar la efectividad de los controles implementados.	Proveedores de Ciberseguridad	Semana 8
	Pruebas de penetración y simulaciones de phishing	Simulación de ataques controlados para evaluar la efectividad de las medidas de prevención.	Proveedores de Ciberseguridad	Semana 8-9
2 Detección	Optimización de infraestructura de seguridad	Implementación de firewalls avanzados, EDR (Endpoint Detection & Response) y políticas de acceso seguro.	Equipo de TI	Semana 9-10
	Implementación de SIEM y monitoreo de eventos	Configuración de herramientas de correlación de eventos.	Seguridad Informática	Semana 9-10
	Análisis de registros y detección de tráfico sospechoso	Monitoreo continuo de logs y redes en busca de anomalías.	Administrador de Sistemas / Redes	Semana 11-12
3 Respuesta	Activación de alertas tempranas	Automatización de notificaciones ante posibles incidentes.	Equipo de Ciberseguridad	Semana 13
	Capacitación a empleados para reportar actividades sospechosas	Sensibilización sobre la importancia de informar incidentes.	Recursos Humanos / Seguridad Informática	Semana 14

Fase	Actividad Clave	Descripción	Responsables	Duración Estimada
	Desarrollo del Plan de Respuesta a Incidentes (IRP)	Elaboración de protocolos de respuesta ante ransomware, incluyendo aislamiento de sistemas y comunicación con las partes afectadas.	Equipo de TI / Consultores	Semana 16-17
4 recuperación	Ejercicios de respuesta ante un ataque de ransomware	Simulación realista de un ataque para evaluar tiempos de respuesta.	CSIRT / Ciberseguridad	Semana 18-19
	Aislamiento de sistemas afectados	Desconexión de dispositivos comprometidos.	Equipo de Seguridad Informática	Semana 15
	Evaluación del alcance del ataque	Determinar los sistemas impactados y datos afectados.	Administrador de Sistemas y Redes	Semana 16

Fuente: Elaboración propia

6.6.2 PRESUPUESTO

La implementación de este plan requiere una inversión significativa, pero es menor en comparación con los costos de recuperación tras un ataque exitoso de ransomware, que puede incluir pérdidas de datos, rescates millonarios y daños a la reputación empresarial. El presupuesto se realizó o diseñó para empresas grandes, con más de 100 empleados, de igual forma se brindan algunas recomendaciones para pequeñas y medianas empresas.

Este esquema de trabajo, alineado con ISO 27001 e ISO 22301, establece una hoja de ruta clara para fortalecer la seguridad y continuidad operativa de las empresas hondureñas ante ataques de ransomware. La integración de estándares internacionales garantiza un enfoque estructurado, probado y alineado con las mejores prácticas para mitigar riesgos y reducir el impacto de los incidentes cibernéticos.

La **metodología de Estimación por Tres Valores (PERT)** permite calcular un presupuesto más preciso al considerar tres escenarios para cada actividad, donde:

- **Optimista (O):** El costo más bajo posible si todo ocurre sin problemas.
- **Más probable (M):** El costo estándar esperado según la experiencia.
- **Pesimista (P):** El costo máximo en caso de complicaciones o sobrecostos.

El **cálculo del costo estimado (CE)** se obtiene con la fórmula de **PERT:**

$$\mathbf{CE} = \frac{\mathbf{O} + (\mathbf{4M}) + \mathbf{P}}{\mathbf{6}}$$

Tabla 18 Presupuesto estimado para el plan

Fase	Concepto	Optimista (O)	Más Probable (M)	Pesimista (P)	Costo Estimado (CE)
Prevención	Auditoría de seguridad y evaluación de riesgos	HNL 51,040.00	HNL 63,800.00	HNL 89,320.00	**HNL 68,061.84**
	Implementación de segmentación de red y restricciones de acceso	HNL 140,360.00	HNL 153,120.00	HNL 191,400.00	**HNL 159,500.00**
	Actualización de software y aplicación de parches	HNL 76,560.00	HNL 89,320.00	HNL 114,840.00	**HNL 93,581.84**
	Configuración de copias de seguridad inmutables	HNL 127,600.00	HNL 140,360.00	HNL 178,640.00	**HNL 146,740.00**
	Capacitación en ciberseguridad y simulaciones de ataque	HNL 76,560.00	HNL 102,080.00	HNL 127,600.00	**HNL 102,080.00**
Subtotal Prevención		HNL 480,618.16			
Detección	Implementación de SIEM y herramientas de monitoreo	HNL 255,200.00	HNL 306,240.00	HNL 370,040.00	**HNL 308,358.16**
	Configuración de IDS/IPS para análisis de tráfico	HNL 178,640.00	HNL 191,400.00	HNL 229,680.00	**HNL 197,780.00**
	Automatización de alertas de seguridad	HNL 63,800.00	HNL 76,560.00	HNL 102,080.00	**HNL 80,821.84**
	Sensibilización en detección de amenazas para empleados	HNL 51,040.00	HNL 63,800.00	HNL 89,320.00	**HNL 65,918.16**
Subtotal Detección		HNL 652,878.16			
Respuesta	Creación del CSIRT y desarrollo del Plan de Respuesta a Incidentes	HNL 102,080.00	HNL 114,840.00	HNL 153,120.00	**HNL 121,220.00**
	Ejercicios de respuesta y simulación de ataques	HNL 114,840.00	HNL 127,600.00	HNL 165,880.00	**HNL 131,861.84**
	Evaluación de impacto y clasificación de activos críticos	HNL 76,560.00	HNL 89,320.00	HNL 114,840.00	**HNL 93,581.84**
	Coordinación con expertos forenses y documentación del incidente	HNL 89,320.00	HNL 102,080.00	HNL 140,360.00	**HNL 104,198.16**
Subtotal Respuesta		HNL 450,861.84			
Recuperación	Restauración de sistemas y recuperación de datos	HNL 127,600.00	HNL 153,120.00	HNL 191,400.00	**HNL 155,238.16**
	Documentación de lecciones aprendidas y mejora de procesos	HNL 51,040.00	HNL 63,800.00	HNL 89,320.00	**HNL 65,918.16**
	Implementación de nuevas medidas de seguridad post-incidente	HNL 102,080.00	HNL 114,840.00	HNL 153,120.00	**HNL 121,220.00**
Subtotal Recuperación		HNL 342,401.84			

Fase	Concepto	Optimista (O)	Más Probable (M)	Pesimista (P)	Costo Estimado (CE)
Total, General (Lempiras)				**HNL 1,926,760.00**	

Fuente: Elaboración propia

Tabla 19 Recomendaciones para Pequeñas y Medianas Empresas

Fase	Recomendaciones
Prevención	Utilizar plantillas gratuitas o herramientas en línea (como el Cybersecurity Framework del NIST) para identificar riesgos comunes sin necesidad de consultores externos.
	Configurar VLANs en routers y switches básicos, y aplicar políticas de control de acceso por roles sin requerir hardware empresarial.
	Establecer un calendario interno de actualizaciones y parches, aprovechando las configuraciones automáticas del sistema operativo.
	Usar servicios como Google Workspace, OneDrive o Dropbox Business con versiones de archivo inmutables, en lugar de soluciones locales costosas.
	Realizar talleres internos mensuales usando videos educativos (por ejemplo, de YouTube o la plataforma CISA.gov) sobre phishing, contraseñas seguras y navegación responsable.
Detección	Implementar soluciones como Security Onion, OSSEC, o incluso el registro de eventos de Windows y alertas básicas del antivirus.
	Utilizar firewalls tipo pfSense con Snort o Suricata como soluciones accesibles para pequeñas redes.
	Configurar alertas básicas en correos o logs de sistemas críticos (como intentos fallidos de acceso) para monitoreo manual.
	Incluir a los empleados en ejercicios de simulación simples (como falsos correos phishing) para fomentar la atención.
Respuesta	No se requiere un CSIRT formal; basta con un encargado que tenga claro el procedimiento básico de aislamiento y respuesta.
	Crear listas de verificación impresas con pasos clave para responder ante incidentes (apagar el equipo, desconectar de la red, informar al responsable).
	Documentar los incidentes y respuestas en hojas de cálculo para análisis posterior.
	Establecer acuerdos con expertos independientes o pequeñas consultoras que puedan brindar apoyo en caso de emergencia.
Recuperación	Verificar regularmente que las copias de seguridad funcionen y se puedan restaurar con facilidad.
	Después de un incidente, documentar qué ocurrió y qué medidas evitarán que vuelva a suceder.
	Reforzar las contraseñas, segmentar mejor, eliminar accesos innecesarios y actualizar lo aprendido tras el incidente.

6.7 CONCORDANCIA

Segmentos de la Tesis con la Propuesta

Para garantizar la coherencia entre los diferentes segmentos de la investigación y la

propuesta planteada, se ha desarrollado la siguiente matriz de concordancia. En ella se relacionan los elementos clave de cada capítulo con los aspectos fundamentales de la propuesta, asegurando que los objetivos, metodologías y hallazgos de la tesis se alineen con la solución presentada.

Tabla 20 Concordancia de los capítulos

Capítulo I			Capítulo II	Capítulo III			Capítulo V	Capítulo VI	
Título de Investigación	**Objetivo General**	**Objetivos Específicos**	**Teorías/ Metodologías de sustento**	**Variables**	**Poblaciones**	**Técnicas**	**Conclusiones**	**Nombre de la Propuesta**	**Objetivos de la Propuesta**
Plan de Contingencia y Respuesta ante Ciberataques de tipo Ransomware en Empresas Hondureñas	Desarrollar un plan de contingencia y respuesta ante ransomware para fortalecer la ciberseguridad en empresas hondureñas.	1. Identificar las principales vulnerabilidades ante ransomware en empresas hondureñas.	- ISO 27001 (Seguridad de la Información)	Variable independiente: Nivel de implementación de medidas de seguridad.	Empresas hondureñas de diferentes sectores que manejan información crítica y dependen de sistemas digitales para su operación.	- Encuesta a responsables de TI y/o con conocimientos sobre tecnología en empresas.	Se evidenció que muchas empresas hondureñas carecen de protocolos adecuados ante ransomware, lo que incrementa el riesgo de pérdidas financieras y operativas.	Plan de Contingencia y Respuesta ante Ransomware para Empresas Hondureñas	1. Diseñar estrategias de prevención para reducir la vulnerabilidad ante ransomware.
		2. Diseñar un plan de contingencia que contemple medidas preventivas, de detección, respuesta y recuperación ante ataques de tipo ransomware.	- ISO 22301 (Gestión de Continuidad del Negocio)	Variable dependiente: Impacto de ransomware en la continuidad del negocio.		- Análisis de incidentes de ransomware en Honduras.			2. Implementar mecanismos de detección y respuesta inmediata.
			- NIST Cybersecurity Framework (Identificación, Protección, Detección, Respuesta y Recuperación)			Revisión documental de mejores prácticas en ciberseguridad	La implementación de un plan de contingencia efectivo basado en estándares internacionales mejoraría la resiliencia empresarial.		3. Establecer protocolos de recuperación para minimizar el impacto de ataques y garantizar la continuidad operativa.
			- Modelos de gestión de riesgos en ciberseguridad.			Entrevistas con expertos en seguridad informática**.**			

Fuente: Elaboración propia

Explicación de la Concordancia

- **El capítulo 1** presenta el problema del ransomware en Honduras, alineándose con la justificación de la propuesta, y se definen los objetivos a alcanzar.
- **El capítulo 2** fundamenta el plan en normativas internacionales (ISO 27001, ISO 22301 y NIST), asegurando un marco regulatorio sólido.
- **El capítulo 3** define la metodología, detallando cada fase del plan, asegurando consistencia con la implementación de la propuesta, en la investigación.
- **El capítulo 5** evalúa y definen las conclusiones que vengan a fortalecer los resultados encontrados.
- **El capítulo 6** analiza la aplicabilidad y se define el plan a trabajar, asegurando una visión a futuro y posibles adaptaciones.

Con esta estructura, se garantiza que cada sección de la tesis mantiene una relación directa y coherente con la propuesta, cumpliendo con los requisitos metodológicos y garantizando su aplicabilidad en el contexto empresarial hondureño.

REFERENCIAS BIBLIOGRÁFICAS

América Latina en 2020: Ataques cibernéticos, sus consecuencias y lo que se avecina. (2020, noviembre 19). https://securelist.lat/america-latina-en-2020-ataques-ciberneticos-sus-consecuencias-y-lo-que-se-avecina/91919/

AO Kaspersky Lab. (2024). *Identificación de ransomware: En qué se diferencian los troyanos de cifrado*. https://latam.kaspersky.com/resource-center/threats/ransomware-attacks-and-types?srsltid=AfmBOorniHi832FoRAT-2XGMq33GCm8MbRk4gOXq_jofHluWd28p7mpg

Ávila Niño. (2023). Ransomware, una amenaza latente en Latinoamérica. *InterSedes, Revista electrónica de las sedes regionales de la Universidad de Costa Rica*, *XXIV*(49), Article 49. https://www.scielo.sa.cr/pdf/is/v24n49/2215-2458-is-24-49-092.pdf

Barrios-Torres, S., & Cáceres-García, J. A. (2022). Economía de defensa: Conceptos generales, asignación de presupuesto y recontextualización. Escuela Superior de Guerra. https://doi.org/10.25062/9786287602069

BID, O. (2020, julio 28). BID-OEA: Aumentan mejoras de ciberseguridad en las Américas, pero aún se necesita trabajo [Informativa]. *BID*. https://www.iadb.org/es/noticias/bid-oea-aumentan-mejoras-de-ciberseguridad-en-las-americas-pero-aun-se-necesita-trabajo#:~:text=Sobre%20el%20BID,a%20d%C3%ADa%20para%20mejorar%20vidas.

Chauhan, S., & Kumar, N. (2015). *Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques.* Elsevier Science & Technology Books.

Check Point Research. (2022). *Cyber Security Report*.

Checkpoint. (2024). Ciber Security Report [Informativa]. *Check Point Research*. https://research.checkpoint.com/

CONATEL. (2020, marzo 21). *Comunicado CONATEL*. CONATEL. https://www.unah.edu.hn/dmsdocument/9669-21032020-cuidado-no-descargue-cualquier-aplicacion-a-su-android-que-le-ofrecen-un-seguimiento-al-tema-del-covid-19

Creswell, J. W., & Poth, C. N. (2018). *Qualitative Inquiry & Research Design* (Fourth edition). SAGE.

Deloitte Global, contact. (2023). *Encuesta mundial sobre el futuro de la cibernética*. 28. https://www.deloitte.com/content/dam/assets-shared/docs/services/risk-advisory/2023/gx-deloitte_future_of_cyber_2023.pdf

Díaz, R. M. (2022). *Ciberseguridad en cadenas de suministros inteligentes en América Latina y el Caribe*. Comisión Económica para América Latina. https://repositorio.cepal.org/server/api/core/bitstreams/2b53c8ee-380e-47de-b115-298e8e06eeaa/content

ESET. (2023). *SECURITY REPORT LATINOAMÉRICA 2023*. 20. www.eset.com/latam

Gartner, Inc. (2024). *¿Cómo organizar tu programa de ciberseguridad?* [Informativa]. https://www.gartner.es/es/tecnologia-de-la-informacion/temas/programa-de-ciberseguridad

Global Cybersecurity Index. (2020). International Telecommunication Union. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Johnson, A., Dempsey, K., Ross, R., Gupta, S., & Bailey, D. (2019). *Guide for security-focused configuration management of information systems* (No. NIST SP 800-128; p. NIST SP 800-128). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-128

Nagar, G. (2024). The Evolution of Ransomware: Tactics, Techniques, and Mitigation Strategies. *Valley International Journal Digital Library*, 1282-1298. https://doi.org/10.18535/ijsrm/v12i06.ec09

NCSI. (2022, octubre 13). *NCSI :: Honduras*. https://ncsi.ega.ee/. https://ncsi.ega.ee/country/hn_1/?selectedCountryIndex=634#details

NICCS. (2024, abril 18). Glosario de palabras y frases comunes en materia de ciberseguridad [Informativa]. *Iniciativa Nacional para Carreras y Estudios en Ciberseguridad*. https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary#explore-terms-a-glossary-of-common-cybersecurity-words-and-phrases

NIST. (2023, noviembre 8). Laboratorio de Tecnologías de la Información [Informativa]. *Centro de recursos de seguridad informática*. https://csrc.nist.gov/glossary/term/US_CERT

Observatorio De La Ciberseguridad. (2020). *Observatorio De La Ciberseguridad En América Latina y El Caribe*. Observatorio De La Ciberseguridad. https://observatoriociberseguridad.org/

Peltier, T. R. (2010). *Information Security Risk Analysis* (3rd ed). Auerbach Publishers, Incorporated.

Ransomware Defense-in-Depth. (2023). CIS. https://www.cisecurity.org/insights/white-papers/ransomware-defense-in-depth

revistaeyn. (2024, febrero 16). *Claro restablece paulatinamente sus servicios en Centroamérica tras ataque ransomware*. www.revistaeyn.com. https://www.revistaeyn.com/empresasymanagement/claro-restablece-paulatinamente-sus-servicios-en-centroamerica-tras-ataque-ransomware-FK17599185

Roberto Hernández Sampieri. (2014). *Metodología de la Investigación* (6.ª ed.).

Sachdeva, S. (2016). Scrum Methodology. *International Journal Of Engineering And Computer Science*. https://doi.org/10.18535/ijecs/v5i6.11

Samaniego Mena, E. A., & Ponce Ordóñez, J. A. (2021). *Fundamentos de seguridad informática*. Editorial Grupo Compás.

Skouby, K. E., Sørensen, L. T., Khajuria, S., & Wireless World Research Forum (Eds.). (2017). *Cybersecurity and privacy: Bridging the gap*. River Publishers.

SOPHOS. (2024, abril). *El estado del ransomware 2024*. https://assets.sophos.com/X24WTUEQ/at/pzm7pw4k5ghvxmfbtcx57mr/sophos-state-of-ransomware-2024-wpes.pdf

Sotres Cruz, P. (2012, septiembre). *ISO 22301 – Continuidad del Negocio*. Product Manager Information Technology. https://www.interempresas.net/FeriaVirtual/Catalogos_y_documentos/87942/Continuidad_Negocio-ISO-22301.pdf

UNIR. (2019, diciembre 11). ¿Qué es la certificación ISO 27001 y para qué sirve? [Academica]. *Universidad en Internet*. https://www.unir.net/revista/ingenieria/iso-27001/

ANEXOS

Anexo 1 Encuesta realizada para recopilar información

1. ¿En qué sector opera su empresa? (Si su sector no está en la lista, no dude en especificarlo) *

- ◯ Finanzas
- ◯ Gobierno
- ◯ Educación
- ◯ Servicio público
- ◯ TI (tecnología de la información)
- ◯ Salud
- ◯ Otras

2. ¿Cuál es el número aproximado de empleados en su empresa? *

- ◯ Entre 1 - 20 empleados
- ◯ Entre 20 - 50 empleados
- ◯ Entre 50 - 100 empleados
- ◯ Más de 100 empleados

3. ¿Cuenta su empresa con un departamento o equipo de ciberseguridad? *

- ◯ Sí, con personal especializado interno
- ◯ Sí, pero tercerizamos el servicio
- ◯ No, la seguridad es gestionada por el equipo de TI
- ◯ No, no tenemos medidas de ciberseguridad específicas

6. ¿Qué medidas preventivas utiliza su empresa contra el ransomware? (Marque todas las que correspondan) *

- [ ] Copias de seguridad regulares
- [ ] Firewalls y sistemas de detección de intrusos
- [ ] Segmentación de red
- [ ] Autenticación multifactor (MFA)
- [ ] Capacitación en ciberseguridad para empleados
- [ ] Software antimalware especializado
- [ ] No tenemos medidas específicas
- [ ] Otras

7. ¿Cada cuánto se actualizan las políticas de ciberseguridad en su empresa? *

- ◯ Cada 6 meses o menos
- ◯ Cada año
- ◯ Cada 2 años o más
- ◯ No contamos con políticas documentadas

8. En caso de un ataque de ransomware, ¿qué acción tomaría su empresa como prioridad? (Clasifique del 1 al 5) *

Pagar el rescate para recuperar la información
Restaurar datos desde una copia de seguridad
Aislar sistemas y contactar a especialistas en ciberseguridad
Reportarlo a las autoridades
No tenemos un plan de acción definido

9. ¿Utilizan sistemas de respaldo de información regularmente? *

- ◯ Sí, diario
- ◯ Sí, semanal
- ◯ Sí, mensual
- ◯ No

10. ¿Cuenta su empresa con un plan de contingencia documentado en caso de ataque de ransomware? *

- ◯ Sí, y ha sido probado con simulacros
- ◯ Sí, pero no ha sido probado
- ◯ No, pero estamos desarrollándolo
- ◯ No tenemos un plan documentado

11. ¿Qué barreras considera que impiden mejorar la ciberseguridad en su empresa? (Marque todas las que correspondan) *

- ☐ Falta de presupuesto
- ☐ Falta de personal especializado
- ☐ Falta de concienciación entre los empleados
- ☐ Falta de apoyo de la alta dirección
- ☐ Desconocimiento de los riesgos
- ☐ Otras

12. ¿Cree que en Honduras existe suficiente concienciación sobre los riesgos del ransomware en el sector empresarial? *

- ◯ Sí, hay un buen nivel de concienciación
- ◯ Algo, pero falta más educación y formación
- ◯ No, hay muy poca conciencia sobre el tema

13. ¿Qué estrategias considera más efectivas para fortalecer la ciberseguridad en las empresas hondureñas? (Seleccione las dos más importantes) *

- ☐ Mayor inversión en tecnología de seguridad
- ☐ Capacitación obligatoria para empleados
- ☐ Regulaciones gubernamentales más estrictas
- ☐ Creación de un centro nacional de respuesta a incidentes
- ☐ Implementación de normas internacionales como ISO 27001 o NIST

14. **Comentarios adicionales:**

Si tiene alguna observación o sugerencia sobre la ciberseguridad, por favor compártala aquí. Su opinión es muy valiosa para nosotros.

Escriba su respuesta

Anexo 2 Entrevista realizada a especialista de ciberseguridad de Checkpoint

1. ¿Cuál es el panorama actual de ataques de ransomware en la región de América Latina, y específicamente en Honduras?
2. ¿Qué características suelen tener los ataques de ransomware que afectan a las empresas de la región? ¿Hay patrones comunes?
3. ¿Qué tan común es que las empresas en Honduras tengan planes de contingencia y respuesta ante incidentes de ransomware?

Preguntas sobre Prevención y Mitigación

4. ¿Cuáles son las estrategias de prevención más efectivas que una empresa puede implementar para reducir el riesgo de ataques de ransomware?
5. ¿Qué papel juegan las políticas de acceso y el control de privilegios en la prevención de este tipo de ciberataques?
6. ¿Qué herramientas o software recomendaría para detectar amenazas de ransomware de manera proactiva?

Preguntas sobre Respuesta a Incidentes

7. ¿Cuáles son los pasos iniciales que debe tomar una empresa en caso de detectar un ataque de ransomware?
8. ¿Existen protocolos de emergencia específicos para minimizar el impacto de un ataque de ransomware en una empresa?
9. ¿Cuáles son los errores comunes que suelen cometer las empresas al responder a un ataque de ransomware?

Preguntas sobre Fortalecimiento y Capacitación

10. ¿Qué tan importante es la capacitación en ciberseguridad para los empleados en la prevención de ataques de ransomware?
11. ¿Recomendaría alguna práctica de simulación de ataques como parte del entrenamiento del personal? ¿Qué tan efectivo es este método?

Preguntas sobre Desafíos y Futuro

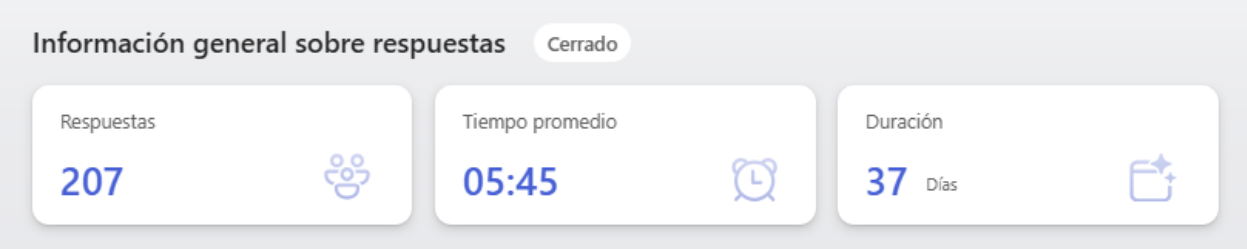
12. ¿Cuáles son los principales desafíos que enfrentan las empresas hondureñas en cuanto a la implementación de medidas de ciberseguridad efectivas contra el ransomware?
13. ¿Cómo anticipa que evolucionarán los ataques de ransomware en los próximos años, y qué medidas deberían tomar las empresas para mantenerse preparadas?

Preguntas sobre Recursos y Soporte

14. ¿Existen recursos públicos o iniciativas gubernamentales en Honduras para ayudar a las empresas en la prevención de ataques de ransomware?

15. ¿Qué recursos o informes de Checkpoint recomendaría para complementar nuestro manual de prevención ante ataques de ransomware?

Anexo 3 Encuesta finalizada



Anexo 4 Importación de Archivo CSV

```python
import pandas as pd
import matplotlib.pyplot as plt
import seaborn as sns  # Para gráficos avanzados
import numpy as np
import textwrap

# Cargar datos
data = pd.read_csv('D://NoteBooks//CsvPruebas//Encuesta_Ciberseguridad_v3.csv')
# Mostrar un preview del grafico
df = pd.DataFrame(data)
display(df)
```

Anexo 5 Análisis de Valores Faltantes

```python
# 3. Análisis de Valores Faltantes
print("\nAnálisis de Valores Faltantes")
print("Valores faltantes por columna:")
print(df.isnull().sum())  # Cuenta los valores faltantes en cada columna

print("\nPorcentaje de valores faltantes por columna:")
print((df.isnull().sum() / len(df)) * 100)  # Porcentaje de valores faltantes

# Visualizar valores faltantes
plt.figure(figsize=(10, 6))
sns.heatmap(df.isnull(), cbar=False, cmap='Blues')  # Mapa de calor de valores faltantes
plt.title('Mapa de Valores Faltantes')
plt.show()
```

Anexo 6 Árbol de Decisión

```python
# Modelo con arbol de decision
from sklearn import tree
from sklearn.tree import plot_tree

modelo_arbol = tree.DecisionTreeClassifier(max_depth=4)
modelo_arbol.fit(X_train, y_train)

plt.figure(figsize=(20,15))
tree.plot_tree(modelo_arbol, feature_names=['Empresa', 'NumeroEmpleados', 'EquipoSeguridad', 'Politicas', 'Respaldos', 'ExistePlanContingencia'],  class_
plt.show()
```

Anexo 7 Regresión Logística

```
from sklearn.linear_model import LogisticRegression
from sklearn.metrics import accuracy_score, confusion_matrix

modelo_logistico = LogisticRegression()
modelo_logistico.fit(X_train, y_train)
precision_modelo = modelo_logistico.score(X_val, y_val)
print(f"Precision: {precision_modelo}")

# Matriz de confusión
y_pred = modelo_logistico.predict(X_val)
cm = confusion_matrix(y_val, y_pred)

# Visualización de la matriz de confusión
plt.figure(figsize=(6,4))
sns.heatmap(cm, annot=True, fmt="d", cmap="Blues", xticklabels=['NoFueVictima', 'SiFueVictima'], yticklabels=['NoFueVictima', 'SiFueVictima'])
plt.xlabel("Predicción")
plt.ylabel("Real")
plt.title("Matriz de Confusión")
plt.show()
```

Anexo 8 Gradient Boosting

```
#Gradient Boosting
from sklearn.ensemble import GradientBoostingClassifier
modelo_gradient_boosting = GradientBoostingClassifier(n_estimators=100)
modelo_gradient_boosting.fit(X_train, y_train)
precision_modelo = modelo_gradient_boosting.score(X_val, y_val)
print(f"Precision: {precision_modelo}")

# Matriz de confusión
y_pred = modelo_gradient_boosting.predict(X_val)
cm = confusion_matrix(y_val, y_pred)

# Visualización de la matriz de confusión
plt.figure(figsize=(6,4))
sns.heatmap(cm, annot=True, fmt="d", cmap="Blues", xticklabels=['NoFueVictima', 'SiFueVictima'], yticklabels=['NoFueVictima', 'SiFueVictima'])
plt.xlabel("Predicción")
plt.ylabel("Real")
plt.title("Matriz de Confusión de Gradient Boosting")
plt.show()
```

Anexo 9 Clustering por K-Means

```
# Aplicar K-Means con 4 clusters (esperando que se relacionen con ser o no víctima)
kmeans = KMeans(n_clusters=4, random_state=42, n_init=10)
clusters = kmeans.fit_predict(X_scaled)

# Agregar los clusters al DataFrame original
train_clean['Cluster'] = clusters

# Comparar clusters con la variable objetivo
cluster_comparison = pd.crosstab(train_clean['VictimaDeRansomware'], train_clean['Cluster'], normalize='index')
print("Relación entre clusters y ser víctima de ransomware:\n", cluster_comparison)

# Visualizar los clusters en función de dos variables relevantes
plt.scatter(X_scaled[:, 1], X_scaled[:, 2], c=clusters, alpha=0.6)
plt.scatter(kmeans.cluster_centers_[:, 1], kmeans.cluster_centers_[:, 2], c='red', marker='X', s=200, label='Centroides')
plt.xlabel('Variable Numero Empleados (Estandarizada)')
plt.ylabel('Variable Equipo Ciberseguridad (Estandarizada)')
plt.title("Clusters en el dataset de ransomware (K-Means)")
plt.legend()
plt.show()
```

Anexo 10 Comparación de Modelos con Curva ROC

```
# PASO 10: Entrenamiento y Comparación de Modelos
models = {
    "Regresión Logística": LogisticRegression(max_iter=1000, class_weight='balanced'),
    "Arbol Decision": tree.DecisionTreeClassifier(max_depth=5),
}

results = []
plt.figure()
for name, model in models.items():
    model.fit(X_train, y_train)
    y_pred = model.predict(X_val)
    proba = model.predict_proba(X_val)[:, 1]

    # Métricas
    accuracy = accuracy_score(y_val, y_pred)
    auc_roc = roc_auc_score(y_val, proba)
    report = classification_report(y_val, y_pred, output_dict=True)

    results.append({
        'Modelo': name,
        'Accuracy': round(accuracy, 3),
        'AUC-ROC': round(auc_roc, 3),
        'Precision (1)': round(report['1']['precision'], 3),
        'Recall (1)': round(report['1']['recall'], 3)
    })
    # Curva ROC
    fpr, tpr, _ = roc_curve(y_val, proba, pos_label=1)
    plt.plot(fpr, tpr, label=f"{name} (AUC = {auc_roc:.2f})")

# Gráfico de Curva ROC
plt.plot([0, 1], [0, 1], 'k--')
plt.xlabel("Tasa de Falsos Positivos")
plt.ylabel("Tasa de Verdaderos Positivos")
plt.title("Curva ROC")
plt.legend(loc="lower right")
plt.show()

# Resultados comparativos
results_df = pd.DataFrame(results).set_index('Modelo')
print("\n=== Comparación de Modelos ===")
print(results_df.sort_values('AUC-ROC', ascending=False))

# PASO 11: Conclusión del Mejor Modelo
best_model = results_df.loc[results_df['AUC-ROC'].idxmax()]
print(f"\nConclusión: El mejor modelo es **{best_model.name}** (AUC-ROC = {best_model['AUC-ROC']})")
```