FACULTAD DE POSTGRADO

TRABAJO FINAL DE GRADUACIÓN

ANÁLISIS DEL SISTEMA DE INFORMACIÓN EN ELCATEX SEGÚN NORMA ISO 27001:2013

SUSTENTADO POR:
JOSÉ MARÍA GARRIDO ÁLVAREZ
JUAN JOSÉ FLORES MURILLO

PREVIA INVESTIDURA AL TÍTULO DE
MÁSTER EN
GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y
GESTIÓN DE OPERACIONES Y LOGÍSTICA

SAN PEDRO SULA, CORTÉS, HONDURAS, C.A.

OCTUBRE, 2022

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTOR

MARLON BREVÉ REYES

SECRETARIO GENERAL

ROGER MARTÍNEZ MIRALDA

VICERRECTOR ACADÉMICO NACIONAL

JAVIER ABRAHAM SALGADO LEZAMA

DIRECTORA NACIONAL DE POSTGRADO

MARIA ROXANA ESPINAL

DIRECTORA NACIONAL DE POSTGRADO

ANA DEL CARMEN RETTALLY

ANÁLISIS DEL SISTEMA DE INFORMACIÓN EN ELCATEX SEGÚN NORMA ISO 27001:2013

TRABAJO PRESENTADO EN CUMPLIMIENTO DE

LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO

DE MÁSTER EN

GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y GESTIÓN DE OPERACIONES Y LOGÍSTICA

ASESOR METODOLÓGICO

JOSÉ RODOLFO SORTO BUESO

ASESOR TEMÁTICO

CARLOS ROBERTO MEJÍA

MIEMBROS DE LA TERNA

LISETTE CÁRCAMO SAUCEDA

JUAN MUÑOZ MAYES

FACULTAD DE POSTGRADO

ANÁLISIS DEL SISTEMA DE INFORMACIÓN EN ELCATEX SEGÚN NORMA ISO 27001:2013

NOMBRES DE LOS MAESTRANDO:

JOSÉ MARÍA GARRIDO ÁLVAREZ

JUAN JOSÉ FLORES MURILLO

RESUMEN

Este trabajo tiene como propósito crear una guía en base a la norma de ISO/IEC 27001:2013 para proteger los activos en ELCATEX, con el objetivo principal de asegurar la cadena de suministro. El proceso metodológico ha sido el de un enfoque mixto con un tipo de alcance descriptivo y el tipo de diseño ha sido el de transversal. La hipótesis nula en nuestra investigación es si el 50% o menos de los ítems de la norma ISO/IEC 27001:2013 se cumple en el ELCATEX. En los últimos años los ciberdelincuentes han generado múltiples ataques a organizaciones de diferentes sectores y tamaños esto a su vez a afectado la continuidad del negocio y reputación de muchas organizaciones. Una nueva tendencia de infiltración y ataques informáticos a las organizaciones sucede a través de la explotación de vulnerabilidades de sus terceros. Se utilizó el método de análisis de brecha para determinar la condición actual en la que se encuentra la empresa en términos de seguridad de la información. Se determinó que existe un 63% de cumplimiento de los requisitos relacionados con la norma. Como conclusión tenemos que gran parte de las organizaciones no están preparadas para gestionar los riesgos ya que no conocen las vulnerabilidades de sus socios, proveedores o clientes. La recomendación principal es dar a conocer a la alta gerencia y su equipo de seguridad informática, una guía que permita la protección de los activos en la empresa.

Palabras claves: Cadena de suministro, Ciberseguridad, Guía, Norma ISO/IEC 27001:2013, Vulnerabilidad.

FACULTY OF POSTGRADUATE

ANALYSIS OF THE INFORMATION SYSTEM AT ELCATEX ACCORDING TO ISO 27001:2013 STANDARD

AUTHORS

JOSÉ MARÍA GARRIDO ÁLVAREZ
JUAN JOSÉ FLORES MURILLO

ABSTRACT

The purpose of this work is to create a guide based on ISO/IEC 27001:2013 standard to protect assets in ELCATEX, with the main objective of securing the supply chain. The methodological process has been that of a mix approach with a type of descriptive scope and the type of design has been transversal. The null hypothesis in our research is if 50% or less of the items of the ISO/IEC 27001:2013 standard is met in the ELCATEX. In recent years, cybercriminals have generated multiple attacks on organizations from different sectors and sizes, this in turn has affected the business continuity and reputation of many organizations. A new trend of infiltration and computer attacks on organizations occurs through the exploitation of third-party vulnerabilities. The gap analysis method was used to determine the current condition of the company in terms of information security. It was determined that there is 63% compliance with the requirements related to the standard of ISO/IEC 27001:2013. As a conclusion, we have that a large part of the organizations is not prepared to manage the risks since they do not know the vulnerabilities of their partners, suppliers, or clients. The main recommendation is to make known to senior management and its computer security team, a guide that allows the protection of assets in the company.

Keywords: Supply chain, Cybersecurity, Guide, ISO/IEC 27001:2013, Vulnerability

DEDICATORIA

Esta tesis se la dedico a mi familia quienes han sido un pilar importante en mi formación profesional y en especial a mis padres Juana Murillo & Juan Ortiz ya que siempre han sido un ejemplo en de constante superación en la vida. A mi mejor amigo Alejandro Ortiz ya que gracias a sus consejos de terminar la maestría es por el cual estoy ya en esta etapa final. Dedico por último a primera jefa que tuve que se llama Dunia Bonilla y que ha sido hasta la fecha un ejemplo de persona por su profesionalismo e inteligencia.

Atte. Juan José Flores Murillo

Dedico este trabajo investigativo a Dios, a mi esposa Alejandra Márquez e hijas Alejandra María y María José, quienes han estado presentes en todo momento para servir de fuente de inspiración, que con su amor y apoyo incondicional me han sabido acompañar, motivar e impulsar a lograr uno de mis más grandes anhelos sin importarles los sacrificios que les ha tocado hacer en función de apoyarme. A la memoria de mi abuelo Juan José Álvarez quien con su legado de humildad y paciencia me mantiene enfocado en lograr mis objetivos.

Atte., José María Garrido Álvarez

AGRADECIMIENTO

Agradezco primeramente a Dios por estar presente en cada etapa de mi vida, por las bendiciones que he recibido y por la sabiduría que me ha dado y por el cual me ha permitido hoy culminar con éxito una meta más en mi vida profesional. A la Universidad Tecnológica Centroamericana (UNITEC), por formarnos como profesionales con visión y excelencia.

Atte. Juan José Flores Murillo

Agradezco plenamente a Dios que me ha permitido superar todas los retos y adversidades para llegar hasta la meta, que ha puesto en mi camino los medios económicos y me ha dado la sabiduría y fortaleza necesaria para no desmayar cuando todo parecía imposible, a mis Padres que han fomentado principios y valores claves para mi vida y formación académica, a mis docentes, compañeros de universidad y de trabajo, amigos y familiares que han formado parte de todo este proceso, a quienes de manera directa o indirecta han aportado a que cada pequeño logro forme parte de lo necesario para llegar a la meta.

Atte. José María Garrido Álvarez

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

Este capítulo presenta la estructura y explica claramente los antecedentes que fundamentan el trabajo de investigación y el origen de este, su importancia, aporte e impacto que pretende generar. De igual forma incluye la definición del problema, su objetivo general, objetivos específicos y preguntas de investigación, así como las acciones propuestas para cumplir con los objetivos del estudio.

1.1 INTRODUCCIÓN

En los últimos años, diversas empresas han comenzado a realizar un proceso de innovación digital, por lo que se requiere del uso de nuevas tecnologías y esquemas almacenamiento de la información en la nube y a la misma vez la disponibilidad en diferentes dispositivos electrónicos. Dicha acción trae muchas ventajas para las empresas, pero también genera ciertas debilidades como es el tener más exposición a riesgos cibernéticos, por lo cual es de mucha importancia que se pueda contar con un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2013 para proteger los datos. Actualmente las organizaciones modernas, han visto la necesidad de involucrarse en la implementación dicha norma como parte de la estrategia del negocio y es así como a la fecha existen un total de 36,362 empresas certificadas a nivel mundial. (León, 2020)

El presente trabajo de investigación tiene como propósito proponer una guía en base a la norma ISO/IEC 27001:2013 para proteger la cadena de suministro en ELCATEX, como respuesta a la creciente necesidad de contar con esquemas de protección de datos y seguridad de la información robustos que permitan asegurar la continuidad del negocio ante los ataques de los ciberdelincuentes.

El concepto de la seguridad informática, toma una perspectiva esencial para las organizaciones en cuanto a su concepción, dado que ya no se maneja simplemente como una serie de herramientas e instrumentos tecnológicos, sino que ya se concibe como un procedimiento de gestión y va mucho más allá de la infraestructura puramente informática, dado que su nombre tiene

un ámbito mucho más vasto- Sistema de Gestión de Seguridad de la Información (SGSI)- es decir comprende la gestión de la seguridad de cualquier tipo de información existente en la organización, lo cual da una perspectiva diferente y pasa de tener una perspectiva tecnológica a una perspectiva empresarial, de negocio, con la tecnología como medio y no como fin.

Con el objetivo de robustecer sus redes de datos, sistemas de información, esquemas de seguridad y minimizar riesgos las organizaciones han invertido muchos recursos en infraestructuras, plataformas tecnológicas y métodos de concientización en sus empleados para que no sean víctimas de la ingeniería social, todo con el fin de minimizar superficies de ataque y que sus redes y sistemas de información no sean vulnerados, sin embargo, también los cibercriminales evolucionan constantemente y modifican sus estrategias de ataque, un ejemplo de ello es la explotación de vulnerabilidades detectadas en terceras partes utilizándolos de puente para llegar hasta sus objetivos principales, comprometiendo considerablemente la confidencialidad, integridad y disponibilidad de la información y operaciones de sus empresas objetivo.

Actualmente ELCATEX no cuenta con la certificación ISO/IEC 27001:2013 y es aquí donde surge la necesidad de proponer una guía que sirva de base para que en un futuro se pueda implementar en dicha empresa. A fin de que tenga éxito dicha actividad es necesario contar con el apoyo de los colaboradores y gerencia y la continua práctica de la guía.

1.2 ANTECEDENTES

En 1834 se registró el primer ciberataque en la historia en donde fue por medio de un telégrafo óptico que tenía dos brazos móviles y que fue inventado por el francés Claude Chappe. Este telégrafo era únicamente usado por el gobierno hasta que dos banqueros sobornaron a un operador para obtener información sobre los movimientos de los mercados nacionales e internacionales. En este caso en específico el operador básicamente emitía información incorrecta y luego al final expresaba un carácter adicional como una señal de que se tenía que eliminar un campo. (García, 2018)

Aproximadamente el 60% de los ataques cibernéticos que sufren las empresas se debe a una mala configuración, conclusión dada luego realizar una encuesta a nivel mundial en el 2021 y en las que participaron alrededor de mil empresas de diferentes sectores en la industria, sin importar el tamaño o giro de la empresa; todas están afrontando desafíos de transformación sin antecedentes por lo que están ante la necesidad de digitalizar los procesos lo más pronto posible. (EFE News Service, 2022)

Cada día es más común ver como las empresas sufren ataques cibernéticos y como resultado afecta drásticamente su cadena de suministro. Según lo señala el Foro Económico Mundial, los delitos cibernéticos aumentaron 151% en el 2021; de los cuales en promedio hubo 270 ataques cibernéticos por organización en donde cada ataque exitoso le cuesta en promedio a una empresa afectada 3.6 millones de dólares.

Las consecuencias y costos de que una empresa sea víctima de un ciberataque y por ende afecte toda su cadena de suministro es elevada. Según Cortés (2007), la implementación de programas de seguridad física y de la información son esenciales en el entorno actual que vive el mundo globalizado, con procesos cada vez más dinámicos. Ciertas medidas de seguridad pueden causar, en un inicio, demoras en los flujos a través de las cadenas de suministro mientras se logran controlar y generalizar las iniciativas de seguridad que están delimitadas por la empresa.

El 72% de las organizaciones cuentan con al menos un incidente de ciberseguridad en los últimos doce meses. Culturalmente en Latino América se cree que los incidentes aumentan conforme aumenta el tamaño de la organización, situación que se descarta en varios estudios a nivel global y regional. Durante este tiempo, el 40.9% de las instituciones consultadas no pueden asegurar cuanto tiempo les tomo normalizar la situación luego de haber sufrido un ataque cibernético. Díaz (2021) comenta que apenas el 4,5% lo logró resolver el incidente en minutos sin embargo a más del 50% de las organizaciones los llevó desde algunas horas hasta más de un mes de esfuerzo retomar la operación habitual. Ciertamente la divulgación de información propia puede impactar en la pérdida de clientes y el paro en las actividades en una empresa.

Uno de los casos más sonados en ataques cibernéticos es el caso de SolarWinds. Fue alarmante este caso ya que decenas de miles de personas de todo el mundo quedaron en peligro ya que el ataque consistía en enviar una supuesta actualización de software a través del programa Orion, que forma parte de SolarWinds. De esta forma lograron infectar los sistemas de las víctimas e introducir un troyano a través del cual poder tener acceso total. Otro caso muy conocido que también ocurrió en el 2021 fue el de la filtración de datos de Twitch. En donde se estima que información sensible como el registro de pago de los usuarios desde 2019 quedaron expuestos al igual que información de sistemas internos de la plataforma, superando los cien gigabytes de información perdida. (Jiménez J. , 2021)

En el momento de examinar las posibles consecuencias de un ataque cibernético, el panorama completo puede resultar un poco difícil de evaluar, ya que además de los posibles daños ocasionados a la información guardada y a los equipos y dispositivos de red, se tiene que tomar en cuenta otros importantes aspectos como ser:

- Horas de trabajo invertidas en las reparaciones y reconfiguraciones de los equipos y redes.
- Pérdidas ocasionadas por la indisponibilidad de diversas aplicaciones es y servicios informáticos: coste de oportunidad por no poder utilizar los recursos.
- Robo de información confidencial y su posible revelación a terceros no autorizados, como ser: formulas, diseños de productos y estrategias comerciales (Gómez, 2017)

Según lo describe Molina & Quintero (2022), en su Tesis de ‘Diseño de un sistema de gestión de seguridad de la información (SGSI) para la empresa Bonos y Descuentos S.A.S, a partir de la norma ISO/IEC 27001:2013” se puede observar que la metodología usada fue la del modelo de proceso PHVA (Planear- Hacer- Verificar- Actuar), junto con la herramienta metodológica de Margerit V3; en cual este último instrumento sirve para identificar los activos de la organización, evaluar las debilidades y proponer decisiones de proteger basado sobre la identificación de Riesgos. Como resultado ante dicho proyecto se obtuvo que mediante los datos del análisis de brecha se determinó que es factible el diseño del SGSI en toda la organización y se realizó una propuesta de mejora de la seguridad como referencia para un futuro.

1.3 DEFINICIÓN DEL PROBLEMA

1.3.1 ENUNCIADO DEL PROBLEMA

A nivel mundial la pandemia ha impulsado el cambio en muchos aspectos sociales, uno de ellos es la manera de hacer negocios como ser el B2B (Business to Business), que consiste en un intercambio comercial entre clientes, proveedores y distribuidores de productos. Por lo regular se manejan altos volúmenes de documentos comerciales que se transmiten entre las empresas y surge el Intercambio Electrónico de Datos (EDI) en un formato común entre sistemas computacionales, por ejemplo, los conocidos como EDIFACT, XML, ANSI ASC X12, TXT. Este servicio permite el intercambio de datos entre sistemas de información y por lo cual se estima que el comercio electrónico B2B alcanzará los 1,8 billones de dólares y representará el 17% de todas las ventas B2B en Estados Unidos en 2023. (Bonde & Bruno, 2019)

Son muchos las áreas de implementación del EDI, en cual podemos mencionar algunos, como ser en el ámbito industrial, financiero, administrativo, o cualquier otro tipo similar de información estructurada, en el que se pueden hacer pedidos, generar facturas, manipular inventarios tanto de materia prima como de producto terminado y revisar catálogos de precios. El flujo natural de esta información genera la necesidad que los sistemas de información interactúen entre sí.

En abril de 2022, Centroamérica enfrenta de forma articulada un inédito ciberataque a Costa Rica, generando impacto a sitios de internet para la declaración de impuestos y también al sistema TICA, con el que se rigen las aduanas para las exportaciones e importaciones de ese país y que tiene contacto con los demás sistemas informáticos nacionales y regionales que permite el tránsito de documentación e información. (Forbes Staff, 2022)

Hoy en día, puede llegar a ser un reto el poder contar con una cadena de suministro segura, ya que la cantidad de individuos u organizaciones que participan en dicha actividad son muchas y esto representa un desafío. Una estrategia completa de seguridad en la cadena de suministro requiere en profundidad los principios de gestión de riesgos y ciberdefensa. Cuando estamos

hablando acerca de la importancia de la seguridad de la cadena de suministro es importante hacer énfasis en dos puntos de vistas, el primero se hace un énfasis en que los ataques a la cadena de suministro tienen como propósito el obstaculizar la logística real; que por lo general solicitan un rescate financiero al final, y el segundo punto de vista es que es solamente un vehículo o un medio para atacar a socios y proveedores que estén conectados. (Avetta Marketing, 2021)

Ante las amenazas permanentes sobre la extracción de datos y entendiendo que esto está presente a nivel mundial, en Honduras La Constitución de la República garantiza en su artículo 76, el derecho a la intimidad personal, familiar y a la propia imagen. Dicho artículo, deja mucho que desear en cuanto al cumplimiento real, ya que, si un hondureño común hace denuncia sobre ello, en muy raras ocasiones se aplica la ley a la persona que violó la intimidad personal o imagen. La rápida afiliación a nuevas tecnologías y el efecto de la pandemia en la rapidez del comercio electrónico, debería de hacer que el gobierno reconsideré el entorno legal para la adecuada defensa sobre nuestros datos. (Zelaya, 2021)

En un 85% la culpa de los ataques cibernéticos es por un error humano, como por ejemplo cuando una persona descarga un juego en su dispositivo móvil en mucho de los casos estas aplicaciones solo tienen la intención de sustraer información privada de las personas. Por lo cual según datos de la revista Cybersecurity Ventures, los gastos para el año 2021 fueron de cerca de $6 billones y de los cuales fueron desglosados de la siguiente manera: Al mes $500,000,00 a la semana $115,400,000 al día $16,400,000 y por segundo de $190,000. (Morales Rojas, 2022)

Estas situaciones colocan a las empresas nacionales en una posición de reflexión sobre su situación individual con relación a la seguridad de la información y la protección de datos, con un enfoque en prevenir situaciones que pudiesen afectar sus operaciones o reputación corporativa, esto nos motiva a generar una Guía para la implementación de un sistema de información de seguridad para el aseguramiento de la cadena de suministro en ELCATEX ya que actualmente la empresa no cuenta con dicha norma.

1.3.2 FORMULACIÓN DEL PROBLEMA

Con el objetivo de enfocar los esfuerzos y recursos de investigación e identificar las variables relacionadas se plantea la siguiente interrogante:

¿Será posible diseñar una guía con base en la norma ISO/IEC 27001:2013 para proteger la cadena de suministro en ELCATEX?

1.3.3 PREGUNTAS DE INVESTIGACIÓN

A continuación, se presentan las preguntas de investigación que favorecen el desarrollo del tema de investigación:

1) ¿Cuál es la situación actual en términos de seguridad de la información y protección de datos en base a la percepción de Gerentes y Directores evaluados en ELCATEX?

2) ¿Cuáles son los aspectos que no están en conformidad con las mejores prácticas de la norma ISO/IEC 27001:2013 en base a la percepción de Gerentes y Directores evaluados en ELCATEX?

3) ¿Qué beneficio puede obtener ELCATEX al momento de la implementar las mejores prácticas de la norma ISO/IEC 27001:2013?

4) ¿Qué propuesta se puede elaborar en términos de protección de datos basado en la norma ISO/IEC 27001:2013?

1.4 OBJETIVOS DEL PROYECTO

Los objetivos tienen como finalidad señalar lo que se pretende hacer en la investigación, es decir nos dictan la ruta a seguir en el trabajo de investigación.

1.4.1 OBJETIVO GENERAL

Diseñar una guía para la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2013 para el aseguramiento de la cadena de suministro de la empresa ELCATEX.

1.4.2 OBJETIVOS ESPECÍFICOS

1) Elaborar una evaluación inicial o diagnóstico en temas relacionados con Seguridad de la Información y protección de datos en base a la percepción de Gerentes y Directores evaluados en ELCATEX.

2) Identificar los aspectos normativos que no están en conformidad con las mejores prácticas de la norma ISO/IEC 27001:2013 en base a la percepción de Gerentes y Directores evaluados en ELCATEX.

3) Establecer los beneficios que la empresa ELCATEX recibirá al implementar las mejores prácticas de la norma ISO/IEC 27001:2013.

4) Elaborar una propuesta para una Guía de Mejores Prácticas en la seguridad de la información y protección de datos basado en la norma ISO/IEC 27001:2013.

1.5 JUSTIFICACIÓN

La importancia del estudio es mostrar como los ataques cibernéticos afectan la cadena de suministro en una empresa y exponer sus consecuencias como tal, cada día se presentan casos donde los ciberdelincuentes intentan vulnerar cierto objetivo por algún periodo de tiempo, pero sin tener éxito. A pesar de ello, estos individuos son constantes y no se dan por vencidos, entonces

buscan organizaciones débiles a nivel de seguridad, que estén vinculadas a su objetivo principal y así mismo ejecutan sencillos ataques informáticos a estas organizaciones vulnerables como pueden ser socios, clientes o proveedores.

Desde el punto de vista social es conveniente realizar este estudio ya que cuando una empresa ha sufrido un ataque cibernético y afectado su cadena de suministro por consecuencia tiene un impacto en su imagen y reputación. Desde el punto de vista financiero es útil este estudio porque muestra como una empresa puede ser impactada en sus procesos de negocios como ser: costos de operación, costos producción, costos de venta y costos de administración. Desde el punto de vista económico**,** es beneficioso el estudio ya que se puede medir y conocer a más detalles cuando existe un robo de información y como afecta a la organización.

Los beneficios del estudio son:

- Resiliencia operativa y ahorro general de costos considerando que los ciberataques cuestan millones de dólares a la economía y tienen un impacto directo las operaciones y capacidades de producción.
- Mayor capacidad para aprovechar los datos para obtener información y tomar decisiones.
- Estrategia de protección contra ataques cibernéticos.
- Cumplimiento de las leyes de privacidad de datos.

CAPÍTULO II. MARCO TEÓRICO

Este capítulo describe el entorno externo e interno que tiene relación con el objeto de estudio previamente establecido en el planteamiento del problema. Se citan las principales fuentes de información consultadas en torno a la investigación.

2.1 ANÁLISIS DE LA SITUACIÓN ACTUAL

En esta sección se aborda la situación actual del entorno del problema planteado, desde el punto de vista internacional (Macroentorno), local (Microentorno) y un análisis de la situación interna de la empresa, por lo cual es necesario conocer datos que puedan ayudar con la investigación.

Independientemente del rubro de la empresa el proceso de certificar un proceso en una empresa implica la ejecución de varias acciones como ser: conocer los requerimientos normativos, examinar la situación de la organización, evidenciar los procesos solicitados por la norma, ejecutar auditorias y registrar el uso del sistema y mejorarlo.

2.1.1 ANÁLISIS DEL MACROENTORNO

Se presenta un breve análisis de países en donde se incluyen datos relacionados con el incremento en ataques cibernéticos impactando la cadena de suministro de las empresas.

2.1.1.1 ASIA

Dentro de los casos de ciberataques reportados en Asia en los últimos años, se puede mencionar lo siguiente.

2.1.1.1.1 JAPÓN

A inicios del 2022, en Japón, se realizó un ciberataque en donde la empresa Toyota fue afectada y por lo cual dicha acción fue realizada desde un proveedor del fabricante de vehículos

Toyota. La consecuencia fue grave y esto hizo que por un día completo se paralizara las catorce plantas de producción de Toyota. En la industria automotriz, cuando un Fabricante de equipos originales, por sus siglas en inglés OEM, para su producción, son miles de dólares en los que es afectado. El proveedor, Kojima Industries, fue objeto de un ataque de "Ransomware" en el que dejó inoperativos a los servidores y se encontraron con un mensaje que estaban solicitando una recompensa a cambio de remover dicho virus. (EFE, 2022) En el anexo 3 podemos observar estadísticas del porcentaje de organizaciones afectadas por Ransomware en el último año. (SOPHOS, 2022)

2.1.1.1.2 TAIWÁN Y COREA DEL SUR

La empresa de comida rápidas, McDonald's, sufrió un ciberataque en donde información confidencial fue sustraída de la base de datos. Afortunadamente, en dicha información no había detalles de pagos, pero si había referencias de correos electrónicos de los clientes y empleados. Dicho ataque al sistema de la empresa fue detectado rápidamente y esto hizo que se evitaran pagar algún rescate por dicha información. En la bolsa de valores, este ataque no paso a más y al día siguiente aumentaron un 1.19% (CriptoSavia, 2021)

2.1.1.2 EUROPA

Dentro de los casos de ciberataques reportados en Europa en los últimos años, se puede mencionar lo siguiente.

2.1.1.2.1 BÉLGICA

Demeestere (2022) menciona que en Bélgica sufrió un ataque cibernético que afectó las terminales petroleras a principios del año dos mil veintidós y que motivo la apertura a una serie de investigaciones judiciales. Dicho ataque hizo que las empresas tuvieran dificultades en cuanto a su operación, como, por ejemplo; los programas de operación de las terminales quedaron invalidas y por ende no se podía descargar mercadería de los barcos. Dicha investigación sostiene una hipótesis que el ataque se debió por motivos criminales o de extorsión.

2.1.1.2.2 ITALIA

Durante el 2021 la región de Lazio, en Roma, Italia, se vio afectado por ciberataques que perturbaron el sistema de reserva de vacunas contra la COVID-19. Dicho ataque fue ejecutado desde el exterior y generó el cierre de la página para reservar cita y el gobierno tuvo que cerrar todos los servidores de los computadores en dicha región. El objetivo principal de dicho ataque era sustraer información personal para luego exigir una recompensa y este último lo solicitaban por medio de Bitcoins. (RPP, 2021)

2.1.1.2.3 ALEMANIA

En el transcurso del 2020 un hospital en Alemania sufrió un ciberataque lo que hizo que tuvieran interrupciones en los servicios de urgencias en las instalaciones, lo cual provocó la muerte de un paciente y en un principio se adjudicó dicha circunstancia como la causa principal de muerte del paciente. Luego de unas investigaciones realizadas por la policía se concluyó que el paciente había llegado en un estado crítico al hospital y que el ciberataque no fue el responsable de la muerte del paciente. Si bien es cierto esto no fue la razón principal de una lamentable muerte, es un tema critico el que los hospitales puedan ser susceptibles a ataques cibernéticos. (O'Neill , 2020)

2.1.1.3 NORTEAMÉRICA

En mayo de 2021 se registró uno de los peores ataques cibernéticos en Estados Unidos, el objetivo fue Colonial Pipeline, oleoducto con sede en Alpharetta, Georgia de los más extensos de Estados Unidos, que se extiende desde Texas hasta Nueva Jersey y que transporta casi la mitad del combustible de aviación y motores que se consume en el noreste de Estados Unidos y gran parte del sur, generando un impacto directo en sus operaciones al tener que parar sus envíos por varios días, poniendo en evidencia las vulnerabilidades de la infraestructura de la organización. (Krauss, 2021). Según indica EFE (2021) Colonial pagó algo más de 4 millones de dólares en bitcoin sin embargo también comparte que finalmente, Colonial no necesitó la herramienta proporcionada por DarkSide para eliminar el encriptado de la información y la compañía se recuperó utilizando respaldos.

En junio de 2021 un ataque cibernético a JBS, el mayor productor de carne del mundo generó impacto en la cadena de suministro a nivel global, forzando el cierre temporal todas sus plantas de carne en Estados Unidos generando un impacto directo a una operación que suministra casi la cuarta parte del suministro de carne estadounidense. (Batista, Hirtzer, & Dorning, 2021)

2.1.1.4 LATINOAMÉRICA

Díaz (2021) menciona que según los datos de CEPAL (Comisión Económica para América Latina y el Caribe) en un estudio publicado en noviembre del 2020 muestra los incidentes de ciberseguridad denunciados y expuestos públicamente en los que se presentan a continuación. De los 30 casos registrados, 11 fueron registrados en el 2020 lo cual si comparamos con el año 2017 representa un incremento del 57%, con el año 2018 un aumento del 83% y para el año 2019 un acrecentamiento del 175%.

Figura 1. Incidentes registrados en logística

Fuente: (Díaz, 2021)

Estos incrementos de casos son preocupantes ya que muestran que tan frágil están los sistemas de información y seguridad en los países latinoamericanos y que se necesitan mejores normas o protocolos que se puedan aplicar para un mejor control.

2.1.1.4.1 ECUADOR

Díaz (2021) indica que el veinte de mayo de dos mil dieciséis hubo un incidente para la organización Banco del Austro en donde el tipo de incidente se describió como vulnerabilidad de día cero en la red SWIFT. Este ataque cibernético represento transferencias monetarias por la red SWIFT y fallas en los controles por parte de la empresa operadora de la red. El impacto cualitativo fue de debilidad del banco por no mantener actualizada la red en cuestión. Otro incidente ocurrió en dicho país el veintiocho de septiembre de dos mil veinte hacia la organización CMA CGM en donde el tipo de incidente se describió como Malware. Este ataque afectó a sus servidores periféricos el lunes 28 de septiembre, lo que impidió que clientes y usuarios ingresaran al sitio web de la naviera y hacer uso de su aplicación. El impacto cualitativo fue de 12 días sitio de e-commerce fuera de servicio.

2.1.1.4.2 MÉXICO

Díaz (2021) señala que el veintiséis de junio de dos mil diecisiete hubo un incidente para la organización APM Terminals México en donde el tipo de incidente se describió como Virus GoldenEyes. Este ataque cibernético represento un acceso a servidores bloqueado. El impacto cualitativo fue que la operación debía realizarse en forma manual, pudiendo solo realizar la descarga de los contenedores. Otro incidente ocurrió en dicho país el veintisiete de junio de dos mil diecisiete hacia la organización Maersk en donde el tipo de incidente se describió como Ransomware Petya. Este ataque cibernético represento un acceso a servidores bloqueado y el impacto cualitativo fue que se afectó a todas las unidades de negocio en Maersk–Envío de contendores. Por último, otro incidente único en México ocurrió el diez de noviembre de dos mil diecinueve hacia la organización Pemex en donde fue atacado cibernéticamente mediante el Ransomware Sodinokibi. Este ataque tuvo un impacto en el acceso bloqueado al 5% del equipamiento y en donde se reportó un impacto cualitativo de $50,000,000.

2.1.1.4.3 ARGENTINA

Díaz (2021) indica que el ocho de junio de dos mil veinte, se reportó un incidente para la organización Light Energía S.A en donde el ataque cibernético fue mediante el Ransomware Sodinokibi y afecto el acceso a servidores y en donde se reporta que tuvo un impacto cualitativo de $14,000.

2.1.1.4.4 CHILE

Díaz (2021) menciona que en Chile se registraron dos incidentes, el primero ocurrió el veinticuatro de mayo de dos mil dieciocho, hacia la organización Banco Estado en donde hubo una vulnerabilidad de día cero en la red SWIFT. La descripción del incidente fue que mientras la institución se encontraba dedicada a la resolución del malware que afectaba a los equipos, los atacantes realizaban transferencias monetarias por la red SWIFT. El impacto cualitativo fue la debilidad del banco por no mantener actualizada la red en cuestión y el impacto cuantitativo fue de $10,000,000. El otro incidente fue reportado el diecisiete de julio de dos mil dieciocho hacia la organización TNT Express ocasionado por el Ransomware Petya en donde afecto el acceso a los servidores. El impacto cualitativo fue de paralización inicial y posteriores retrasos en el servicio de entrega que impactó en la facturación y en donde el impacto cuantitativo fue de $300,000,000. Cabe mencionar que este incidente también afecto países como: Brasil, Argentina y Perú.

2.1.1.4.5 COSTA RICA

En abril de dos mil veintidós Costa Rica informo la afectación en todos sistemas aduaneros y de pago de impuestos producto de un ciberataque, paralizando los servicios digitales de estas entidades, considerado como un ataque articulado e inédito en la región centroamericana, teniendo que activar un plan de contingencia para asegurar los flujos del comercio en la región. El grupo Conti se atribuyó la acción y pidió 10 millones de dólares a cambio de no divulgar la información que extrajo del Ministerio de Hacienda. (Forbes Staff, 2022)

A finales de mayo de dos mil veintidós se reportan en Costa Rica varios problemas en los sistemas de información de la Caja Costarricense del Seguro Social (CCSS), esto generando un

impacto directo a nivel nacional en las operaciones de hospitales y el acceso al Expediente Digital Único en Salud (EDUS) de todos sus afiliados, teniendo que recurrir a procesos de consulta manual. (Cabezas, 2022)

2.1.1.6 PAÍSES CON MAYOR NÚMERO DE CERTIFICADOS CON LA NORMA ISO/IEC 27001:2013.

La siguiente tabla muestra un resumen del Top 10 de países certificados con la norma ISO/IEC 27001:2013.

Tabla 1.Ranking de Países con certificación ISO/IEC 27001:2013

Ranking	País	Numero de certificados
1	Japón	7170
2	Reino Unido	2259
3	India	2170
4	China	2002
5	Italia	970
6	Rumania	893
7	Taiwán	779
8	España	701
9	Estados Unidos	664
10	Alemania	640

Fuente: (Daruma, 2016)

2.1.2 ANÁLISIS DEL MICROENTORNO

Honduras no cuenta con un equipo nacional dedicado solamente a la ciberseguridad, pero cuenta con un órgano regulador que supervisa el sector de las telecomunicaciones y este es la Comisión Nacional de Telecomunicaciones (CONATEL). La única ley existente para proteger la ciberseguridad se aplica solamente a las redes sociales y es llamada Ley de Estrategia de Ciberseguridad Nacional con prevención de campañas de odio y discriminación en redes sociales. Aunque Honduras no cuenta con una legislación general en materia de privacidad ha publicado leyes, muy por el contrario, inmunizando a las autoridades estatales de responsabilidad en las investigaciones penales. (IPANDETEC Centroamérica, 2018)

Es importante mencionar que el nuevo código penal en Honduras si cataloga varios delitos cibernéticos como ser: piratería, phishing, robo de identidad, pornografía y provocación sexual pero lastimosamente en el país aun cuando un ciudadano vaya a denunciar dichos actos estos no se ejecutan debido a un sistema corrupto que ha existido por varias décadas en el país.

Las leyes sobre la ciberseguridad en Honduras son escasas y las que fueron creadas en el Congreso Nacional no toman en cuenta a todos los actores como ser: informáticos, sociedad civil y defensores de derechos humanos. Como lo menciona Raudales (2017) en el artículo de "La brecha existente en la ciberseguridad en Honduras" durante el Informe de Ciberseguridad 2016 por parte del Observatorio de la Ciberseguridad en América Latina y el Caribe, a nivel mundial, da como resultado una matriz del Índice Mundial de Ciberseguridad y muestra que Estados Unidos encabezaba con 0.824 y que apenas en Centro América, Costa Rica se ubicaba en la posición#17 con 0.353. Honduras junto a otros ocho países, compartían el último lugar de la clasificación con un índice de 0.000.

Durante el reporte del 2020 sobre la medición del EGDI (Índice de Gobierno Digital) coloca a Honduras en la posición #138 de los 139 miembros de las Naciones Unidas. Este índice, EGDI, lo componen tres características que son: Índice de Infraestructura de Telecomunicaciones, Índice de Capital Humano e Índice de servicio en línea. La puntuación obtenida en el 2020 fue la más baja desde una comparación desde hace veinte años; por lo tanto, este retroceso es un indicador que en Honduras se deben aplicar mejores leyes para poder contar con un mejor desempeño. Otro indicador que se puede mencionar que analiza la brecha digital en Honduras, es el NRI, Índice de Disposición de Red, en el cual se muestra que para el año 2016, el país se ubicaba en la posición #94 de los 139 miembros evaluados. Dicha puntuación obtenida fue de 3.7 sobre los 7 que es lo máximo que pueden obtener; lo que quiere decir que la ejecución efectiva por parte del gobierno en cuanto a este tema es de apenas un 53%. (Escoto & Jipsion, 2021)

Tabla 2 Rangos EGDI de Honduras

Año	2003	2004	2005	2008	2010	2012	2014	2016	2018	2020
Rango	124	113	115	110	107	117	114	127	123	138

Fuente: (Escoto & Jipsion, 2021)

La ciberseguridad en América Latina tiene muchos aspectos por mejorar de manera general. La metodología NSCI, que por sus siglas en ingles significa National Cyber Security Index, está compuesta por doce indicadores y uno de ellos es la respuesta a ciberdelincuentes por parte de equipos de emergencia informática ante ciber incidentes. En dicho indicador, evalúa a Honduras con una puntuación de cero; lo cual es muy triste para el país. Los países con mejor puntuación son Colombia, Perú y Chile. Dicho análisis también indica que, de manera universal en la región, carece una contribución global a la ciberseguridad, delimitación de amenazas y la protección de servicios esenciales; en lo cual esta última está relacionada con servicios como ser: electricidad, agua y drenaje. A continuación, se presenta una figura de la ponderación global de los países de América Latina en base a información recabada en el 2019. (Aguilar Antonio, 2021)

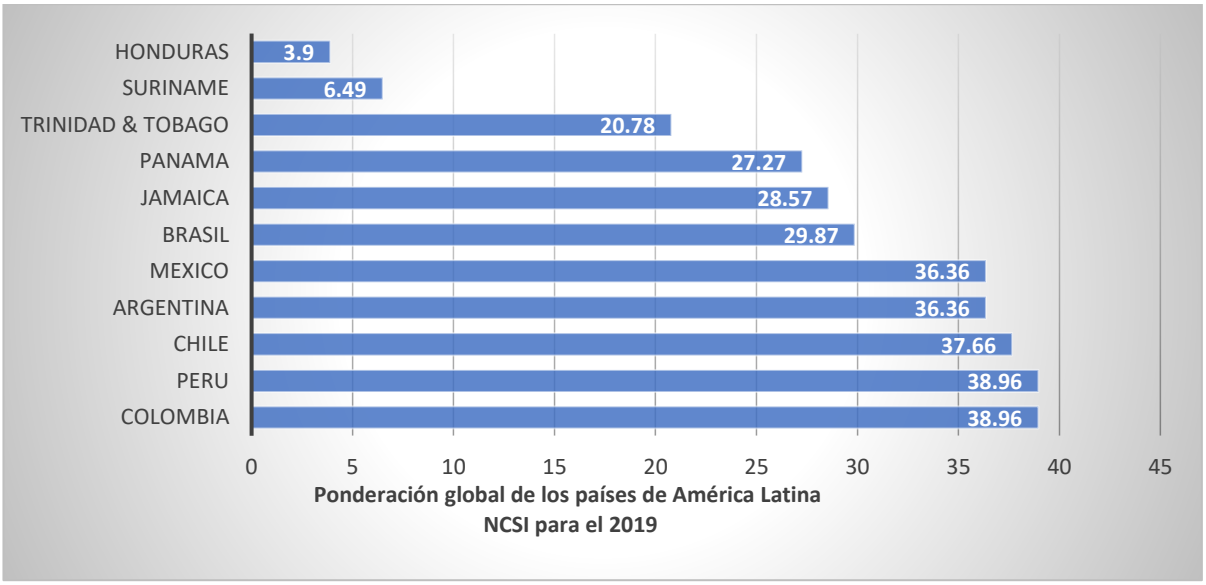


Figura 2. Ponderación global de los países en América Latina

Fuente (NCSI, 2019)

2.1.3 ANÁLISIS INTERNO

ELCATEX es una empresa dedicada a la fabricación de tela de punto, piezas cortadas y programas de paquete completo en donde cuenta con un área de 500.000 pies cuadrados y es capaz de producir hasta dos millones de libras por semana. Inicio sus operaciones en 1984 y tiene por objeto el establecimiento en Honduras de un centro textil integrado, el cual ofrecería productos de alta calidad para ambos, los mercados nacionales e internacionales. La base de clientes incluye

empresas muy reconocidas como JC Penney, SanMar, Nordstrom, Dickies y HBI, y la variedad de productos incluye camisetas básicas, programas de ropa interior, sudadera de felpa con gorro y zipper, camisetas polo de piqué para hombres, mujeres y niños.

En un análisis interno, la empresa ELCATEX, tiene un enfoque directo sobre el crecimiento del negocio, innovación, atendiendo las nuevas exigencias del mercado y estableciendo nuevas formas de operar, ya que cuenta con excelencia operacional, generando valor con calidad, eficiencia y tiempos de respuesta, costos y flexibilidad. ELCATEX mantiene de forma permanente apego directo a sus principios operacionales los cuales al igual que su estrategia corporativa están plasmados en su cuadro de mando integral, ver anexo 4 y anexo 5. (ELCATEX, 2020)

ELCATEX se caracteriza por tener una fortaleza en recurso humano y formación, por lo cual está consciente que la educación es clave para cambiar el presente y el futuro de todo ser humano por lo cual ELCATEX promueve programas educativos para sus empleados y para las comunidades. Hasta la fecha, cuentan con 200 graduados de IHER, 80 becas todos los años y 85 alianzas con universidades. Cuentan también con el "Programa de Educación Acelerada" en el cual apoyan a los colaboradores con estudios secundarios gratis y se apoyan con materiales y aulas acondicionadas. Por último, es valioso detallar que la empresa ELCATEX tiene un compromiso por la innovación en los procesos cuyos impactos sean ecológicos por lo cual desde el 2010 se ha invertido en equipos eficientes lo cual ha logrado una reducción del 70% en el uso del agua en 10 años. Los factores mencionados y entre otros, hacen que la cultura organizacional sea positiva.

ELCATEX al formar parte de uno de los Grupos Corporativos más grandes a nivel nacional cuenta con una infraestructura tecnológica muy robusta apalancada por marcas de alto nivel de calidad, utilizando esquemas de trabajo de vanguardia que soportan la demanda de sus operaciones y la sinergia que estas tienen con las personas y procesos, sin embargo como todo tiene oportunidades de mejora especialmente en la estandarización y apego que las normas y mejores prácticas de los Sistemas de Gestión de Seguridad de la Información demandan para fortalecer las cultura de seguridad que cada recurso en la compañía debe adoptar para reducir la brecha del típico 2% que los equipos y herramientas tecnológicos no pueden cubrir como lo es el factor humano.

En un análisis externo, ELCATEX se ve amenazado por carecer de certificaciones en tema de seguridad de la información, aspecto que hoy en día es de mucha importancia ya que como se ha visto en párrafos anteriores, ha habido innumerables casos de ataques cibernéticos. Actualmente las únicas certificaciones que cuenta la empresa son: WRAP (Worldwide Responsible Accredited Production) y OEKO-TEX (Certificado que verifica que no existan sustancias nocivas ni en los textiles, ni en las fases de la fabricación de un determinado producto) y también con CT-PAT (Customs-Trade Partnership Against Terrorism) que tiene como finalidad garantizar la seguridad en las distintas áreas de la cadena de suministro y protegerla en contra del terrorismo por parte del gobierno de los Estados Unidos.

2.1.3.1 MISIÓN, VISIÓN Y VALORES EMPRESARIALES

La Misión y Visión es en esencia la declaración de principios de la empresa, por lo tanto, en ELCATEX se define como lo siguiente:

a) MISIÓN- Ser la organización de manufactura textil referente a nivel mundial.

b) VISIÓN- Liderar una cultura de mejora continua a través de procesos, productos y servicios innovadores que maximicen el valor para nuestros clientes asegurando la sostenibilidad y desarrollo integral de nuestros colaboradores.

c) VALORES:
    a. Competitividad
    b. Responsabilidad
    c. Desarrollo
    d. Calidad

2.2 TEORÍA DE SUSTENTO

A continuación, se exponen conceptos y teorías en general que se consideran valiosos para enmarcar correctamente la investigación y sirven de sustento teórico.

2.2.1 CADENA DE SUMINISTRO

Terrado (2007) menciona que una cadena de suministro es el conjunto de actividades que son necesarias para poder llevar a cabo el proceso de venta de un producto en su totalidad. La gestión de la cadena de suministro se tiene que cumplir correctamente para garantizar la satisfacción de los clientes. La cadena de suministro comprende desde la obtención de la materia prima mediante diferentes proveedores, la fabricación y producción del material, el transporte y logística del producto ya terminado, el almacenamiento del producto terminado, la venta del producto en donde se usan diferentes canales de distribución y por último la facturación y la entrega de dicho producto.

2.2.2 SGSI

Un Sistema de Gestión de la Seguridad de la Información o SGSI por sus siglas, es el elemento más importante de la norma ISO/IEC 27001:2013 ya que contempla un proceso sistemático para la protección ante cualquier riesgo o peligro, que podría llegar a impactar la confidencialidad e integridad de la información. Sabiendo que uno de los principales catalizadores para la eficiencia de un negocio es la información y que garantizar que esta sea precisa, se mantenga segura y esté disponible para quien debe tener acceso es determinante. (ISO27000.ES, 2005)

Cada organización requiere establecer sus propias políticas y objetivos para garantizar la seguridad de la información de la compañía. Es importante que se pueda coordinar las actividades de protección para contribuir en el aseguramiento de la seguridad de la información especialmente cuando es sabido que toda la información almacenada y procesada por una organización está expuesta ante la amenaza de ataque cibernéticos ya sea por intereses comerciales, intelectuales, chantaje y extorsión o también por amenazas asociadas a errores intencionados o por negligencia,

están las amenazas asociadas a fallos técnicos en los sistemas de almacenamiento de datos, sistemas de información y redes de comunicación. (ISO27000.ES, 2005)

Una vez que la gerencia en una empresa ha identificado sobre los objetivos en cuanto a la seguridad de la información es necesario establecer los mecanismos que nos van a ayudar para poder cumplir con dichos objetivos. Una vez implementado el SGSI en una empresa, se podrán observar beneficios tales como: Avalar un alto nivel de confidencialidad, integridad y disponibilidad de la información, contar con un factor diferenciador que creara un plus ante la competencia y los actores como ser proveedores y clientes tendrán mayor confianza debido a la calidad y confidencialidad que se genera al implementar dicho sistema. (ISO27000.ES, 2005)

2.2.3 EL CICLO DE MEJORA CONTINUA

El ciclo de mejora continua está implícito en la norma ISO/IEC 27001:2013 y las fases del ciclo de mejora continua están divididas en cuatro. La primera fase comprende la etapa de planeación, en donde acá se planifica la implantación del SGSI y se determina el contexto de la organización, se definen los objetivos y las políticas que permitirán alcanzarlos. La segunda fase es la de ejecución, en esta se implementa y pone en funcionamiento el SGSI. Se ponen en práctica las políticas y los controles, para ello debe de disponerse de procedimientos, asegurando la capacitación necesaria para ello, todos estas políticas y controles surgen de un análisis de riesgos previamente ejecutado. La tercera fase consiste en la monitorización y revisión del SGSI. Se controla la aplicación de los procedimientos y el aseguramiento de cumplimiento de objetivos propuestos de manera eficiente. Y la última fase es en donde se toman acciones de mejora en el SGSI, ejecutando acciones correctivas para rectificar o mejorar brechas detectadas en las fases anteriores.

En todo diseño de un SGSI es clave tener presente la aplicación de un proceso de mejora continua, por lo que se recomienda partir con una primera versión del ciclo adaptado a las necesidades, operativas y recursos de la organización, con unas medidas de seguridad mínimas que permitan proteger la información y cumplir con los requisitos de la norma. De esta manera el sistema de gestión de seguridad de la información será mejor adoptado por los involucrados,

evolucionando de manera progresiva y con un esfuerzo menor. (Gómez Fernández & Fernández Rivero, 2018)

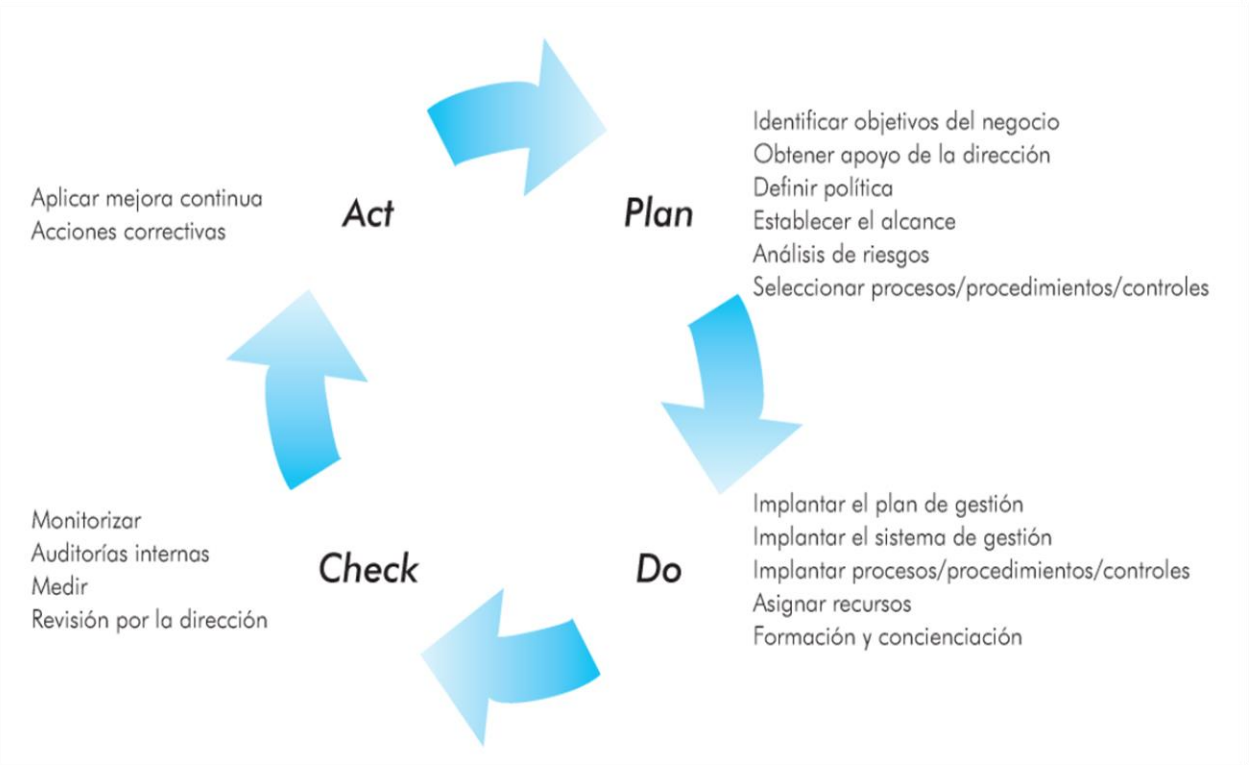


Figura 3. Ciclo PDCA

Fuente: (Gómez Fernández & Fernández Rivero, 2018)

2.2.4 CIBERSEGURIDAD

Según lo afirma Guardeño, Martínez, Encinas (2020) la ciberseguridad la podemos definir como "el conjunto de técnicas, procedimientos y protocolos encaminados a la protección de la información vinculada a los usuarios de las ciber tecnologías" (p. 12).

Arroyo (2020) comenta que el tipo de amenaza que más puede afectar a un usuario particular es fundamentalmente aquella que a través del engaño clásico, intenta hacer ver al usuario que alguien es fiable y por lo tanto ese usuario acaba haciendo lo que el atacante quiere. Lo que se hace en el contexto ciber no es nuevo, lo que sí es nuevo es el modo de hacerlo; por lo ejemplo: la propaganda, distorsión, generación de ansiedad y por último llevar al usuario a una situación de incertidumbre.

2.2.5 GESTIÓN DE RIESGOS

La Gestión de Riesgo es el proceso que se ejecuta para definir y gestionar los riesgos a los que puede estar expuesto la organización. En toda organización y manera general se puede decir que el riesgo ha estado presente de manera permanente, en ese sentido, medirlo y gestionarlo de manera correcta siempre ha sido importante. Debido al constante crecimiento de las organizaciones y a la dependencia que las diferentes actividades económicas generan de los factores tecnológicos, indistintamente de cuál sea su sector de actividad cada organización está obligada definir procesos de medición y gestión del riesgo. (Población García, 2013)

Los riesgos de una organización normalmente dividen en dos tipos; el primero de ellos es el riesgo sistémico en el cual es un riesgo innato al propio mercado y que afecta en mayor o menor grado a todos los activos existentes en la economía. Por ejemplo, el incremento en los intereses afecta de manera negativa a todos los actores en una empresa. El segundo tipo de riesgo que puede existir en una organización es el riesgo idiosincrático, es el riesgo que afecta exclusivamente a un sector en especifico (Población García, 2013)

2.2.6 ISO/IEC 27000

Se público el 1 de mayo de 2009, y desde entonces ha tenido diferentes revisiones, una segunda edición en diciembre de 2012, una tercera en enero de 2014 y una cuarta en febrero de 2016, en esta última versión no se incluye el ciclo de Deming para evitar convertirlo en el único marco de referencia que se puede utilizar para el mejoramiento continuo que forma parte inherente de la norma. Esta norma proporciona las bases y definiciones que es necesario comprender para determinar la importancia que tiene para una organización la implementación de un Sistema de Gestión de Seguridad de la Información, permite delimitar su alcance y el propósito de implementarla. (ISO27000.ES, 2005)

2.3 CONCEPTUALIZACIÓN

En esta sección se detallan los conceptos específicos de las variables tomados en cuenta para el trabajo de investigación.

2.3.1 SEGURIDAD CIBERNÉTICA o CIBERSEGURIDAD

Según lo afirma Martín (2020), se conoce como ciberseguridad a la práctica de preservar los dispositivos, sistemas, redes y datos de ataques u otros fines maliciosos. Entre las amenazas más comunes de un ciberataque incluye: Estafas por correo electrónico, amenazas internas y los ataques de intermediario. La ciberseguridad trata de trabajar en robustos sistemas que sean idóneos de operar antes, durante y después.

2.3.2 DEFINICIÓN DE UN SGSI

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es un conjunto de procesos que permiten establecer, implementar, mantener y mejorar de manera continua la seguridad de la información, tomando como base para ello los riesgos a los que se enfrenta la organización. Su implantación supone el establecimiento de procesos formales y una clara definición de responsabilidades en base a una serie de políticas, planes y procedimientos que deberán constar como información documentada. (Gómez Fernández & Fernández Rivero, 2018, p. 22)

2.3.3 LIDERAZGO

Para poner en marcha un SGSI es fundamental contar con el liderazgo y compromiso de la dirección, siendo este uno de los epígrafes contemplados en la norma, ya que el cambio de cultura que genera el proceso sería imposible de lograr sin la implicación constante de la dirección. Entre otras cosas, la dirección deberá demostrar su compromiso, aportando los recursos necesarios, tanto económicos como humanos. (Gómez Fernández & Fernández Rivero, 2018, p. 22)

2.3.4 POLÍTICA

La política de seguridad de la información es un documento en donde la organización adquiere el compromiso de implantar y mejorar de manera continua el sistema de gestión. Este debe ser socializado a todos los empleados y partes interesadas de la organización, incluyendo clientes y proveedores.

> Es la información documentada en la que se reflejan, en términos generales, los objetivos de la organización en materia de seguridad de la información y las principales líneas de acción que permitan proteger su información frente a pérdidas de confidencialidad, integridad y disponibilidad. (Gómez Fernández & Fernández Rivero, 2018, p. 23)

En el documento se consideran los aspectos de negocio relacionados su giro, aspectos legales, contractuales y de cumplimiento regulatorio.

2.3.5 ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN

Para asegurar el cumplimiento de los procedimientos es determinante asegurar que se tenga claro quién debe realizarlos, de esta manera se garantiza que cada uno comprende su responsabilidad.

> Para que esta designación sea clara y no se ponga en duda, debe ser determinada por la dirección, que además debe asegurarse de que los roles sean comunicados. La definición de responsabilidad permite a la dirección asegurar que se cumplen los requisitos de la Norma UNE-EN ISO/IEC 27001:2013, así como mantenerse informada sobre el comportamiento del sistema de gestión de la seguridad de la información. (Gómez Fernández & Fernández Rivero, 2018, p. 23)

Es por ello por lo que conocer la organización e identificar todos los niveles jerárquicos es sumamente importante para asegurar el que los objetivos de negocio sean comprendidos por todos los miembros de la organización. (Gómez Fernández & Fernández Rivero, 2018, p. 23)

2.3.6 TRATAMIENTO DE LOS RIESGOS

La ejecución de un plan de tratamiento de riesgos de seguridad de la información es una de las partes más complicadas de la implementación de la norma ISO/IEC 27001:2013. Según los parámetros establecidos por la empresa, se comienza identificando los niveles de riesgos y determinar cuáles son aceptables y cuáles no. Existe una posibilidad en el que el riesgo puede llegarse aceptar y por ende la empresa decide convivir con él; sabiendo que no le impactara significativamente sus operaciones. Una vez que este identificado el riesgo, en el proceso de tratamiento de riesgo; se procede a una acción de analizarlo, evaluarlo y por último seleccionar opciones de tratamiento de riesgo; entre los que pueden estar: eliminando por completo el riesgo, realizar una modificación al riesgo y transferir el riesgo a un tercero. (Gómez Fernández & Fernández Rivero, 2018)

2.3.7 SELECCIÓN DE CONTROLES

Para el tratamiento de los riesgos identificados es necesario seleccionar controles de seguridad que permitan el tratamiento de riesgos, diseñarlos según sea necesario o seleccionarlos de alguna fuente. Los controles seleccionados deben ser comparados con los que la Norma UNE-EN ISO/IEC 27002 (Anexo A de UNE-EN ISO/IEC 27001:2013) contiene, para validar que no se han excluido controles necesarios.

> A la hora de valorar la aplicación de un control se debe considerar hasta qué punto permitirá reducir el riesgo y cuál va a ser el coste de su implementación y mantenimiento. Puede darse el caso de que un control que ayude a reducir el nivel de riesgo sea demasiado costoso o difícil de implementar frente a los beneficios que aporta, siendo por lo tanto viable excluir dicho control. El coste de implementación y mantenimiento de un control nunca debería superar a los beneficios que se esperan de él. (Gómez Fernández & Fernández Rivero, 2018, p. 27)

2.3.8 GESTIÓN DE RIESGOS

Una vez seleccionados los controles se repetirá el análisis de riesgos, teniendo en cuenta ya todas las medidas de seguridad implementadas (riesgo actual) y aquellas planificadas (riesgo residual), que deberán figurar en un plan de tratamiento de riesgos de la seguridad de la información. El propietario del riesgo debe aprobar el valor de riesgo aceptable, asumir el riesgo residual y aprobar el plan de tratamiento de riesgos. (Gómez Fernández & Fernández Rivero, 2018, p. 27)

2.3.9 EVALUACIÓN Y DESEMPEÑO

Una vez implantados los procesos en la organización, es necesario darle continuidad mediante procesos de monitoreo y control para asegurar el cumplimiento y la mantención de estos a lo largo del tiempo y que el sistema este brindando los resultados esperados con base en los indicares o métricas que previamente se han definido como parte de los parámetros de medición o puntos de control. Adicional a estos puntos de control es importante tener en cuenta las auditorías internas y las revisiones constantes por parte de la dirección como parte de la evaluación de cumplimiento del sistema de gestión. (Gómez Fernández & Fernández Rivero, 2018)

2.3.10 MEJORA CONTINUA

Es una actividad recurrente para incrementar la capacidad del sistema de gestión, siendo un requisito básico de acuerdo con todas las normas ISO. Como sabemos estas aportan herramientas para conseguir la mejora continua del sistema, por ejemplo, auditorías internas, revisión por dirección, acciones correctivas, entre otras, adicionalmente la implantación de controles, la gestión de incidentes de seguridad, que aportará información para la prevención de incidencias y para mejorar el funcionamiento de la organización (Gómez Fernández & Fernández Rivero, 2018, p. 34)

2.3.11 CONCIENCIACIÓN Y FORMACIÓN DEL PERSONAL

Determinar las competencias necesarias para el personal que realiza tareas en aplicación del SGSI y satisfacer dichas necesidades por medio de formación o de otras acciones. Evaluar la eficacia de las acciones realizadas manteniendo registros de estudios, formación, habilidades, experiencia y cualificación. (ISO27000.ES, 2005, p. 1)

2.4 INSTRUMENTOS

A continuación, se describen los instrumentos que otros autores han utilizado en investigaciones previas en cuanto al tema de la seguridad de la información basado en la norma ISO/IEC 27001:2013.

2.4.1 METODOLOGÍA OCTAVE

La metodología OCTAVE (Operational Critical, Threat, Asset and Vulnerability Evaluation) hace uso del conocimiento de varios niveles de la organización en una empresa y se enfoca en: identificar los elementos críticos y las amenazas a esos activos; por lo cual Hurtado (2011) manifiesta que es un instrumento de evaluación de riesgo desarrollado por la SEI (Software Engineering Institute) en Estados Unidos. Dicho instrumento fue desarrollado para ser implementado en organizaciones que cuentan con más de 300 empleados y que se encuentra dividido en tres etapas: (1) Desarrollan perfiles de amenaza basado en los activos, (2) Identificar vulnerabilidades de la infraestructura tecnológica y (3) Desarrollar estrategias y planes de seguridad.

2.4.2 NIST SP 800-300

El instrumento NIST 800-300 es una guía para la administración de riesgos en tecnologías de la información, divulgado por el Instituto Nacional de Estándares y Tecnología. Como lo afirma, Ruiz (2019), los estándares de NIST deben de ser cumplidos por todos los productos y servicios que de alguna forma dependen de alguna tecnología. La finalidad del instrumento es de suministrar una base para el desarrollo de la gestión de riesgo. Dicha metodología está compuesta por 9 pasos básicos para el análisis como ser:

- Fase 1- Caracterización del sistema.
- Fase 2- Identificación de activos.
- Fase 3- Identificación de vulnerabilidades.
- Fase 4- Análisis de controles.
- Fase 5- Determinación de probabilidad.
- Fase 6- Análisis del impacto.
- Fase 7- Determinación del riesgo.
- Fase 8- Recomendaciones de Control.
- Fase 9- Documentación de resultados.

2.4.3 MATRIZ DE RIESGO

La matriz de riesgo es una herramienta de gran provecho que ayuda a gestionar y controlar los riesgos que puedan presentarse en la operación o en la implementación de servicios; frente a lo cual Moisés (2014) manifiesta que: el concepto de riesgo es utilizado desde el punto de vista de la economía de la empresa, para expresar la incertidumbre sobre los eventos y sus resultados que podrían tener un efecto negativo en el rendimiento de la organización y en sus objetivos. El riesgo puede definirse como una función de: riesgo = *f (*evento, probabilidad, impacto)

Tabla 3. Matriz de Riesgo

Impacto	Extremadamente improbable	Muy improbable	Probable	Muy probable	Extremadamente probable
Muy alto	3	3	4	5	5
Alto	3	3	3	4	5
Moderado	2	3	3	3	4
Bajo	1	2	3	3	3
Mínimo	1	1	2	3	3

Probabilidad

Fuente: (Jiménez M. , 2020)

2.4.4 MATRIZ SOA

Según lo manifiesta Parrado (2020) la declaración de aplicabilidad (SoA, por sus siglas en inglés, Statement of Applicability) de la norma ISO/IEC 27001:2013, de Sistemas de gestión de Seguridad de la información (SGSI), es un documento formado por la relación completa de los controles de seguridad de la información evaluables, que se indican en la norma. El documento SoA puede registrarse en el formato que más le conviene a la empresa, pero lo más importante es su contenido, que generalmente incluirá:

- Controles del estándar.
- Si aplican o no y sus justificaciones.
- Su estado de implementación.
- Documentación relacionada (Procedimientos, evidencias, etc.)

2.4.5 ANÁLISIS DE BRECHA

Según lo manifiesta Grupo Fraga (2018) el análisis de brechas en ISO/IEC 27001:2013 nos indica la distancia a la que se encuentra la organización del cumplimiento de los requisitos y controles de la norma. El análisis de brechas no nos informa sobre los problemas o posibles problemas que se puedan presentar. Dicho análisis no es un requisito obligatorio para certificarse en la norma, pero es una herramienta estratégica. Por lo general se cuenta con seis pasos para realizar el análisis de brecha ISO/IEC 27001:2013.

- Revisar los requisitos de la norma
- Diseñar el cuestionario de cumplimiento
- Determinar el nivel de madurez del cumplimiento
- Analizar los resultados
- Elaborar el informe de resultados
- Construir el plan de acción.

2.5 MARCO LEGAL

En toda nación existe una constitución que rige todos los actos relacionados con el poder de las instituciones o los habitantes. A esto le precede una serie de códigos, reglamentos y normas de índole fiscal, comercial, civil y penal y finalmente existe una serie de reglamentaciones regionales o locales casi siempre bajo los mismos aspectos; frente a lo cual Hernández (2019) menciona que la situación actual en Honduras en cuanto al marco legal es el siguiente:

- El país no cuenta con un equipo nacional de ciberseguridad que defienda al país de la ciberdelincuencia.
- El país no cuenta con una estrategia de ciberseguridad.
- No existe una ley que regule la protección de datos personales.
- El país no es suscritor de convenios o tratados contra la ciberdelincuencia.
- Los delitos cibernéticos no están debidamente tipificados en la legislación.
- El Instituto Hondureño de Ciencia, Tecnología y la Innovación es el ente estatal especializado en TICs (Tecnología de información y Comunicación)

CAPÍTULO III. METODOLOGÍA

En este capítulo se detalla las estrategias de metodología de estudio. El diseño de la investigación tiene como intención definir el proceso mediante el cual se obtendrá información para responder las preguntas de investigación y concluir si la hipótesis planteada se acepta o se rechaza.

3.1 CONGRUENCIA METODOLÓGICA

3.1.1 MATRIZ METODOLÓGICA

Rivas (2015) afirma:

> La matriz metodológica se define como el instrumento científico que permite hacer congruente y coherente el proceso de la medición de variables independientes, creando un marco de comparación racional y ordenado para la construcción de un cuestionario. (p. 204)

Todos los proyectos de investigación se basan en variables. Según lo detalla, Pino (2010) la variable independiente es aquella que el experimentador modifica a voluntad para averiguar si sus modificaciones provocan o no cambios en las otras variables. En consecuencia, la variable independiente ejerce influencia en otras variables llamadas dependientes. Las variables dependientes actúan como efecto de una causa que ejerce coerción y son estas las que designan las variables a explicar. La identificación de las variables es importante ya que va a proporcionar enfoque al proyecto de investigación. Por lo tanto, a continuación, primero se detalla un Diagrama de Variable y posterior se presenta la Matriz de Congruencia Metodológica.

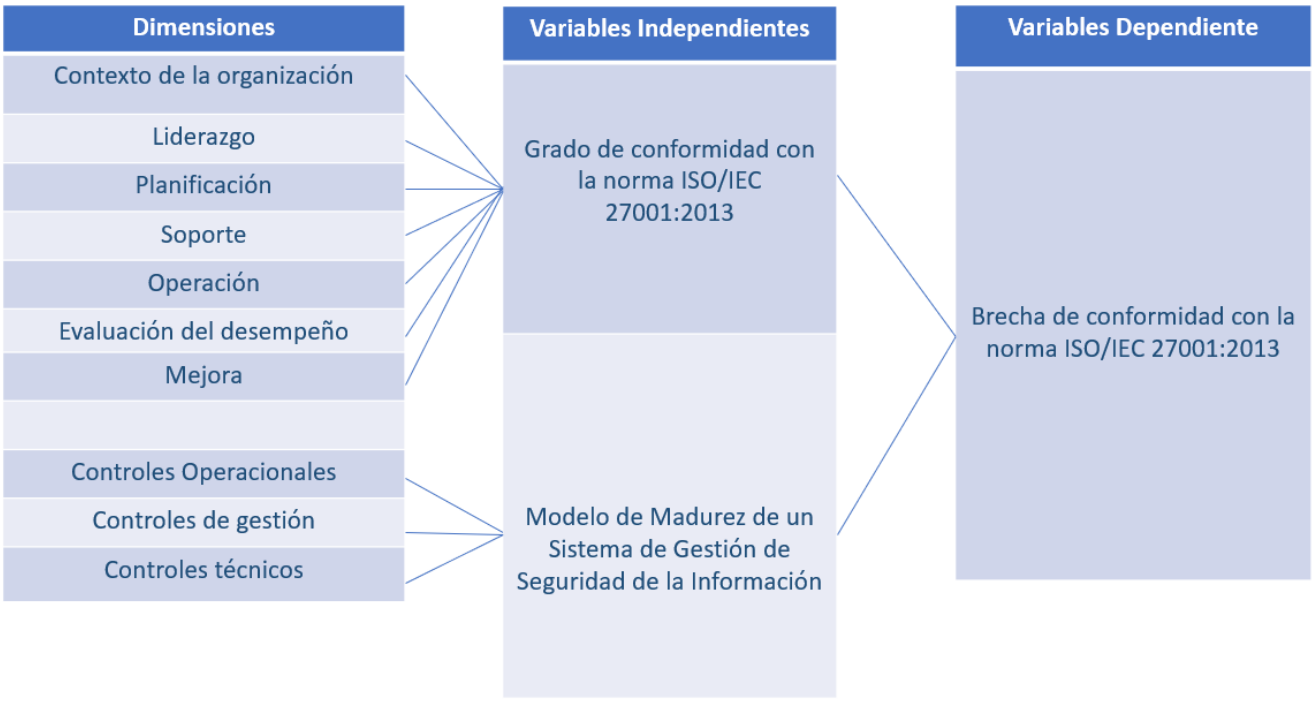


Figura 4. Diagrama de variables

Elaboración: Fuente propia

En la matriz de congruencia metodológica se puede contemplar una relación existente entre el problema planteado y el objetivo general. Según lo plantea Soto (2018), la dimensión puede denominarse una subvariable, por lo cual en conjunto se detalla el comportamiento de la variable en estudio y los indicadores es la cuantificación numérica de las dimensiones.

Tabla 4. Matriz de congruencia metodológica

Titulo	Análisis del sistema de información en ELCATEX según norma ISO 27001:2013				
Problema		**Objetivos**		**Variables**	
	Preguntas de Investigación	**General**	**Específicos**	**Independientes**	**Dependiente**
¿Será posible diseñar una guía con base en la norma ISO/IEC 27001:2013 para proteger la cadena de suministro en ELCATEX?	¿Cuál es la situación actual en términos de seguridad de la información y protección de datos en base a la percepción de Gerentes y Directores evaluados en ELCATEX?	Diseñar una guía para la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2013 para el aseguramiento de la cadena de suministro de la empresa ELCATEX.	Elaborar una evaluación inicial o diagnóstico en temas relacionados con Seguridad de la Información y protección de datos en base a la percepción de Gerentes y Directores evaluados en ELCATEX	Grado de conformidad con la norma ISO/IEC 27001:2013	Brecha de conformidad
	¿Cuáles son los aspectos que no están en conformidad con las mejores prácticas de la norma ISO/IEC 27001:2013 en base a la percepción de Gerentes y Directores evaluados en ELCATEX?		Identificar los aspectos normativos que no están en conformidad con las mejores prácticas de la norma ISO/IEC 27001:2013 en base a la percepción de Gerentes y Directores evaluados en ELCATEX		
	¿Qué beneficio puede obtener ELCATEX al momento de la implementar las mejores prácticas de la norma ISO/IEC 27001:2013?		Establecer los beneficios que la empresa ELCATEX recibirá al implementar las mejores prácticas de la norma ISO/IEC 27001:2013	Modelo de madurez de un SGSI	
	¿Qué propuesta se puede elaborar en términos de protección de datos basado en la norma ISO/IEC 27001:2013?		Elaborar una propuesta para una Guía de Mejores Prácticas en la seguridad de la información y protección de datos basado en la norma ISO/IEC 27001:2013		

Fuente: Elaboración propia

3.1.2 OPERACIONALIZACIÓN DE LAS VARIABLES

A continuación, se describen las variables que se identificaron en la presente investigación en donde se definen cada una de ellas y el proceso consiste en convertir las variables en indicadores de medición que serán analizados y estudiados como parte de la investigación.

Tabla 5. Operacionalización de las variables

Variable Dependiente	Variable Independiente	Definición		Dimensión	Indicador	Técnica	Preguntas	Respuestas	Escala
		Conceptual	Operacional						
Brecha de conformidad con la norma ISO/IEC 27001:2013	Grado de conformidad con la norma ISO/IEC 27001:2013	Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.	Herramienta para determinar el grado de implementación de un sistema de gestión de seguridad en ELCATEX	Contexto de la organización	Nivel de satisfacción de las necesidades y expectativas de las partes interesadas	Encuesta	Preguntas 1-53	Dicotómicas	Nominal
					Nivel de conformidad del alcance del SGSI				
				Liderazgo	Nivel de compromiso de la alta gerencia				
					Roles, responsabilidades y autoridades en la organización.				
				Planificación	Nivel de Efectividad de las acciones para tratar los riesgos				
					Nivel de consistencia en los objetivos de seguridad y su planificación para conseguirlos				

Fuente: Elaboración propia

Continuación Tabla 5. Operacionalización de las variables

Variable Dependiente	Variable Independiente	Definición		Dimensión	Indicador	Técnica	Preguntas	Respuestas	Escala
		Conceptual	Operacional						
Brecha de conformidad con la norma ISO/IEC 27001:2013	Grado de conformidad con la norma ISO/IEC 27001:2013	Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.	Herramienta para determinar el grado de implementación de un sistema de gestión de seguridad en ELCATEX	Soporte	Nivel de aprovisionamiento de los elementos necesarios para la operación	Encuesta	Preguntas 1-53	Dicotómicas	Nominal
					Nivel de recursos, competencias profesionales, estructura de decisión y de comunicación.				
				Operación	Margen errores humano				
					Margen de fallas electrónicas				
					Margen desperfectos en equipos electrónicos				
				Evaluación del desempeño	Nivel de seguimiento continuo en plazos definidos.				
					Nivel de análisis/evaluación por la dirección para asegurar que funcione lo planificado				
				Mejora	Nivel de obligaciones cuando la organización encuentra no conformidad				
					Nivel de importancia para la organización de mejorar continuamente la adecuación/eficacia del SGSI				

Fuente: Elaboración propia

Continuación Tabla 5. Operacionalización de las variables

Variable Dependiente	Variable Independiente	Definición		Dimensión	Indicador	Técnica	Preguntas	Respuestas	Escala
		Conceptual	Operacional						
Brecha de conformidad con la norma ISO/IEC 27001:2013	Nivel de madurez de un SGSI	Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.	Indicador que muestra el grado de madurez de un SGSI en una organización.	Controles Operacionales	Nivel medio de madurez	Entrevista	Preguntas 1-39	Likert 1. Totalmente desacuerdo 2. En desacuerdo 3. Neutral 4. De acuerdo 5. Totalmente de acuerdo	Nominal/ Ordinal
				Controles de gestión			Preguntas 40-68		
				Controles técnicos			Preguntas 69-117		

Fuente: Elaboración Propia

3.1.3 HIPÓTESIS

Según lo define Galicia (1998), la hipótesis es una proposición respecto a algunos elementos empíricos y otros conceptuales y sus relaciones mutuas, que surgen más allá de los hechos y las experiencias conocidas, con la intención de llegar a una mayor comprensión de estos.

Dado que en ELCATEX no se ha realizado previamente un análisis de la norma ISO 27001:2013, se ha definido las siguientes hipótesis:

H_O: El 50% o menos, de los ítems de la norma ISO/IEC 27001:2013 se cumplen en ELCATEX en base a la percepción de Gerentes y Directores evaluados.

Hi: Más del 50%, de los ítems de la norma ISO/IEC 27001:2013 se cumplen en ELCATEX en base a la percepción de Gerentes y Directores evaluados.

3.2 ENFOQUE Y MÉTODOS

Según lo afirma Hernández-Sampieri, Fernández, C & Baptista (2010) existen tres enfoques que se pueden realizar en la metodología de la investigación y esos son: enfoque cuantitativo, cualitativo y mixto. El enfoque cuantitativo cuenta con las características de: utilizar estadísticas, prueba de hipótesis y hace un análisis de causa-efecto, mientras que el enfoque cualitativo explora los fundamentos en profundidad, los significados se extraen de los datos y no se fundamenta en la estadística y por último el enfoque mixto es una combinación entre el cuantitativo y el cualitativo.

Al usar como técnicas de recolección de datos una encuesta con respuestas dicotómicas y la entrevista (Juicio de expertos), se definió un enfoque cualitativo.

3.3 DISEÑO DE LA INVESTIGACIÓN

En esta sección se detalle acerca del diseño de la investigación. Christensen (1980) afirma que "el termino diseño se refiere al plan o estrategia concebida para obtener la información que se desea" (p. 100)

El diseño marca al investigador lo que se debe de hacer para conseguir los objetivos de estudio, contestar las interrogantes que se han trazado y analizar la hipótesis expresada. Es por eso, que a continuación se muestra el diagrama resumen de la investigación.

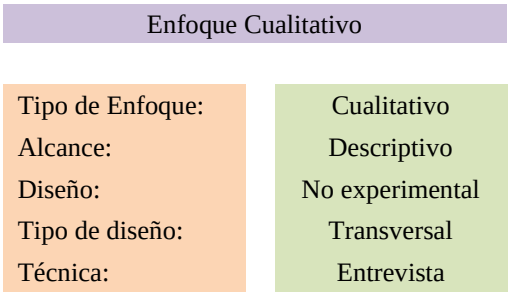


Figura 5: Diagrama resumen de la investigación

Elaboración: Fuente propia

3.3.1 UNIDAD DE ANÁLISIS

Se denomina unidad de análisis al "conjunto o grupo de personas, empresas, instituciones o cosas que son sujetos de estudio de la investigación que se realiza" (Bernal, 2016, p. 116)

Por ende, en base a ello en el desarrollo del presente estudio, la unidad de análisis se conforma por los colaboradores, que han realizado las responsabilidades dentro de ella y por las condiciones físicas de la instalación. La distribución de los colaboradores es la siguiente:

a) Departamento de Tecnología: Director de Tecnología
b) Departamento de Finanzas: Contralor Financiero
c) Departamento de Auditoria: Auditor de Sistemas
d) Departamento de Compras: Director de Compras
e) Departamento de Importaciones y Exportaciones: Gerente de Área
f) Departamento de Servicio al Cliente: Gerente de Área
g) Departamento de Producción: Gerente de Operaciones
h) Departamento de Planificación: Gerente de Área
i) Departamento de Materia Prima: Gerente de Área
j) Departamento de Desarrollo Organizacional: Gerente de Área
k) Departamento de RRHH: Gerente de Área

3.3.2 POBLACIÓN

"Una población es el conjunto de todos los casos que concuerdan con determinadas especificaciones". (Hernández Sampieri, Collado, & Baptista, 2014, p. 174).

La población en esta investigación está dada por 11 personas de alta gerencia, en donde tienen las siguientes características:

- Género: Femenino o Masculino
- Edad: Un rango entre 30 años – 60 años
- Nivel Educativo: Grado académico mínimo de Ingeniería o Licenciatura

- Ocupación: Gerentes y directores
- Horario de trabajo: Administrativo; de 7:30 am – 5:30 pm

.

3.3.3 MUESTRA Y TÉCNICAS DE MUESTREO

"La muestra es, en esencia, un subgrupo de la población. Digamos que es un subconjunto de elementos que pertenecen a ese conjunto definido en sus características al que llamamos población" (Hernández Sampieri, Collado, & Baptista, 2014, p. 175)

Dado que la población de interés es un número pequeño de personas, en la presente investigación, se estableció que la muestra será igual a la población y por lo tanto cuenta con las mismas características poblacionales, como se ha mencionado en párrafos anteriores.

3.3.4 UNIDAD DE RESPUESTA

Para la presente investigación, la unidad de respuesta está basado en la conformidad de lo establecido en la norma ISO/IEC 27001:2013 y en lo cual se detalla lo siguiente:

a) En cuanto a la conformidad: La norma ISO/IEC 27001:2013 contiene 114 controles de seguridad de la información que están divididos en 14 secciones y de los cuales son "obligaciones" que es necesario cumplir. Por lo tanto, las inconformidades son la guía para crear un sistema de información seguro.

3.4 TÉCNICAS E INSTRUMENTOS APLICADOS

3.4.1 INSTRUMENTOS

Los instrumentos de investigación son los recursos que el investigador puede utilizar para abordar el problema detallado y extraer información de ellos. Por el cual, se detallan a continuación los instrumentos usados en esta investigación:

A) Análisis de brecha sobre la seguridad de la información

Según lo indica, González (2016), el análisis de brecha es una herramienta de análisis para comparar el estado y desempeño real de una organización, estado o situación en un momento dado, respecto a uno o más puntos de referencia seleccionados de orden local, regional, nacional y/o internacional.

Para obtener un informe inicial sobre el cumplimiento de la norma se procederá a realizar un análisis de brecha por lo cual en el siguiente Capítulo IV se mostrarán los resultados de la encuesta aplicada para poder medir el grado de cumplimiento de los controles de la norma con base en la medición de la percepción del grupo de interés. La encuesta cuenta con preguntas relacionadas a las siete dimensiones de la norma ISO/IEC 27001:2013:2013.

B) Análisis de nivel de madurez de un SGSI

Los modelos de madurez de un SGSI buscan decretar una valoración estandarizada, con la que se pueda decretar el estado de la seguridad de la información en una organización, y que nos permita poder proyectar el camino que se tiene que recorrer para obtener las metas de seguridad deseadas. Estos niveles de seguridad son progresivos, de tal forma que la seguridad de la información implementada aumente conforme se incremente los niveles de madurez. Se procederá a realizar dicho análisis en base a una entrevista realizada a personas debidamente seleccionada en base a su perfil y cuyas preguntas fueron obtenidas en base al anexo A de la norma ISO/IEC 27001:2013.

3.4.2 TÉCNICAS

El propósito de las técnicas de investigación es la adquisición de datos necesarios para el estudio del problema objeto de investigación. Las técnicas que se aplicaron en el presente trabajo de investigación son las siguientes:

a) Encuesta

Tamayo & Tamayo (2003) afirma que la encuesta es aquella que permite dar respuestas a problemas en términos descriptivos como de relación de variables, tras la recogida sistemática de información según un diseño previamente establecido que asegure el rigor de la información obtenida.

Para la presente investigación se aplicó, la encuesta de 'Test de cumplimiento de ISO/IEC 27001:2013' a una población seleccionada y en el cual está compuesta por 53 preguntas en torno a las siete dimensiones de la norma ISO/IEC 27001:2013. El tipo de respuestas en la encuesta fue de tipo dicotómicas ya que pertenecen a variables categóricas y al usar una encuesta de este estilo significa que la investigación es cualitativa.

b) Entrevista

Alonso (1994) afirma que la entrevista se construye como un discurso expresado principalmente por el entrevistado por que comprende las intervenciones del entrevistador cada uno con un sentido fijo. Aplicando esta técnica se permite realizar un sondeo en temas de interés y profundizar con respecto a temas en específicos. Y por último nota, el investigador puede obtener información adicional que no estaba considerada en un inicio del estudio.

Para la presente investigación se aplicó la entrevista para poder determinar el grado de madurez del SGSI que ELCATEX tiene basado en la percepción de los entrevistados. El anexo A de la norma ISO (Gutiérrez, 2021)O/IEC 27001:2013:2013 contiene 14 controles que fueron usados para poder ejecutar dicha técnica. Las personas que fueron seleccionadas y que ayudaron a contestar preguntas en los Controles, fueron los siguientes:

- A7 Seguridad en los Recursos Humanos – Gerente de RRHH
- A15 Relación con los Proveedores – Director de Compras

- A6 Organización de la Seguridad de la Información. A14 Adquisición, desarrollo y mantenimiento de sistemas de información y A16 Gestión de incidentes de seguridad de la información – Director de Tecnología
- A8 Gestión de Activos, A10 Criptografía, A12 Seguridad en las Operaciones, A13 Seguridad en las Comunicaciones – Director de Tecnología y Gerente de Planta
- A9 Control de Acceso – Gerente de Planta
- A5 Políticas de Seguridad de la Información y A17 Gestión de la Continuidad del Negocio – Contralor Financiero, Auditor de Sistemas, Gerente de Import/Export, Gerente de Servicio al Cliente, Gerente de Planificación, Gerente de Materia Prima y Gerente de Desarrollo Organizacional.

3.5 FUENTES DE INFORMACIÓN

3.5.1 FUENTES PRIMARÍAS

Las fuentes primarías son además llamadas fuentes de primera mano y son aquellos recursos documentales que han sido publicados por primera vez, sin ser filtrados, resumidos, o interpretados por algún individuo. Este tipo de fuentes se proceden de la actividad investigativa de los seres humanos. Entre las características de una fuente primarías es: Son originales, son evidencia directa para una investigación y son muy valiosas para todas las disciplinas. (Gonzales, 2019)

En este caso de investigación se utilizaron las siguientes fuentes primarías:

a) Encuesta aplicada a toda la población en donde los resultados se verán reflejados en el Capítulo IV.
b) Entrevista a personal seleccionado en el cual tiene un nivel amplia experiencia con el tema.

3.5.2 FUENTES SECUNDARIAS

Las fuentes secundarias son textos basados en fuentes primarías e implican generalización, análisis, síntesis e interpretación del tema. Dicha fuente, está diseñada para facilitar y maximizar el acceso a las fuentes primarías.

En este caso de investigación se utilizaron las siguientes fuentes secundarias:

a) CRAI/ Bases de datos, libros electrónicos
b) Páginas web de organismo internacional como ISO
c) Tesis de “Guía de implementación de Sistema de Gestión de Calidad y Buenas Prácticas de Manufactura en la Fábrica de Pastas de San Pedro Sula” sustentado por Loly Gutiérrez.

CAPÍTULO IV. RESULTADOS Y ANÁLISIS

En este capítulo se detallan los resultados obtenidos de la aplicación de los instrumentos de medición para determinar el grado de conformidad que tiene ELCATEX según lo establecido en la norma ISO/IEC 27001:2013:2013 esto en función de la percepción del grupo de personas que conforma nuestras fuentes primarias sobre el cumplimiento de los controles de la norma.

4.1 INFORME DE PROCESO DE RECOLECCIÓN DE DATOS

En esta investigación se usó un formato de formulario que está en la misma norma ISO 27001 a la cual fue aplicada a la población de estudio y por ende se concluye que el instrumento ya está validado.

A pesar de lo anterior, se desarrolló un proceso de validación de contenido por juicio de expertos con el propósito de asegurar que la misma era adecuada para aplicarla en ELCATEX (Ver Anexo 6). También se realizó una medición de fiabilidad usando Alfa de Cronbach para las 19 preguntas que se miden en escala de Likert (Ver Anexo 7) y se detalla a continuación:

- Validación por juicio de expertos.
    - Tres personas con amplio conocimiento en el tema aprobaron la encuesta. Ver Anexo #6: Formato de Validez de contenido de instrumento de recolección de datos.
    - Entre las observaciones iniciales que se realizaron a la encuesta fue: Dar una introducción breve a la encuesta, pregunta (3) recomienda actualizar palabras de ‘partes internas y externas’ por ‘agentes internos y externos’. Pregunta (7), actualizar las siglas SGS a SGSI, pregunta (50) recomienda cambiar la palabra ‘implica’ por la palabra ‘involucra’

- Realización de una prueba piloto.
    - La prueba piloto se realizó a tres personas a las que no pertenecen a la muestra seleccionada, pero si a la población con características similares. Dicha prueba piloto fue aplicada a:
        - Jefe de Soporte Sistemas Grupo ELCATEX
        - Gerente Corporativo de Infraestructura Grupo ELCATEX
        - Gerente Corporativo de Desarrollo Grupo ELCATEX
    - La encuesta tiene un total de 53 preguntas.

- Evaluación de resultados obtenidos.
    - La fiabilidad de la escala en el instrumento de la encuesta fue el siguiente:
        - Consistencia- El cálculo del coeficiente de Cronbach fue de 0.802. En el Anexo 7 se podrá ver el análisis restante de los datos que fueron usados en el programa SPSS Statistics.
            - Dado que se obtuvo un coeficiente de Cronbach mayor a 0.7, podemos concluir que la encuesta es consistente.

El proceso de recolección de datos para la encuesta de "Test de Cumplimiento ISO 27001" fue el siguiente:

1. Creación de encuesta en Microsoft Forms ya que es una herramienta que permitirá ver los resultados de una manera inmediata.
2. Enviar el enlace de la encuesta a la población seleccionada por medio del correo electrónico.
3. Esperar entre cinco a siete días hábiles en obtener respuestas de toda la población.
4. Tabular los datos de la encuesta para realizar el análisis.

El proceso de recolección de datos que se usó para la entrevista con el propósito de medir el cumplimiento de los catorce controles del Anexo A de la norma ISO 27001 estuvo basado en la realización de preguntas dirigidas a los diferentes responsables de las áreas involucradas en dar

respuesta a los grupos de control pertinente y estas fueron gestionadas mediante correo electrónico y vía llamada telefónica, haciendo uso de un formulario digital.

4.2 RESULTADOS Y ANÁLISIS DE LAS TÉCNICAS APLICADAS.

ELCATEX fue sometida a una evaluación diagnóstica para establecer el grado de conformidad que posee actualmente en base a los lineamientos detallados en la norma ISO/IEC 27001:2013 y la percepción que los Gerentes y Directores encuestados tienen sobre el cumplimiento de los controles de la norma. Dicha evaluación se llevó a cabo por medio de siete secciones y que en promedio muestra un grado de conformidad global del 63% el resultado se puede encontrar en el Anexo 8: Encuesta de Cumplimento de Norma ISO/IEC 27001:2013.

El detalle de la encuesta con su respectiva sección de acuerdo con la norma ISO/IEC 27001:2013, es el siguiente:

- La Organización y su Contexto- Ocho preguntas
- Liderazgo- Nueve preguntas
- Planificación- Ocho preguntas
- Soporte- Diez preguntas
- Operación- Ocho preguntas
- Evaluación y desempeño- Siete preguntas
- Mejora- Tres preguntas

A continuación, se muestra la operación matemática y la secuencia en las que estas deben ejecutarse a fin de determinar el porcentaje global con respecto a la norma ISO/IEC 27001:2013.

1. Convertir todos los “Si” en un “1” y los “No” en un “0”
2. Realizar la sumatoria de “1” por cada pregunta en cada sección.
3. Realizar una sumatoria global de la sección.
4. Detallar el total máximo (11 encuestados x el total de preguntas en cada sección)
5. Obtener un porcentaje global por sección.

El Anexo 9: Resultados de la Encuesta de Cumplimiento de Norma ISO/IEC 27001:2013 se encontrará el detalle de la operación matemática por cada sección.

El nivel de madurez según el cumplimiento ISO/IEC 27001:2013 es el siguiente:

- Inexistente- Porcentaje de cumplimiento 0%
  - No se encuentran implementados.
- Inicial- Porcentaje de cumplimiento 1-20%
  - Se han implementado bajo una necesidad específica y ocasional sin evidencia documentada.
- Repetible- Porcentaje de cumplimiento 21-40%
  - Se han implementado y existe un procedimiento. Pero no están completamente documentados
- Definido- Porcentaje de cumplimiento 41-60%
  - Se han implementado y documentado totalmente en procedimientos, políticas y estándares.
- Administrado- Porcentaje de cumplimiento 61-80%
  - Se mantiene control sobre su eficacia y rendimiento.
- Optimizado- Porcentaje de cumplimiento 81-100%
  - Se han establecido acciones que han logrado su mejora continua y óptimo cumplimiento.

A continuación, se detalla el grado de cumplimiento por cada sección o dimensión de la norma ISO/IEC 27001:2013, junto con su % de brecha lo cual va a representar el estado actual en ELCATEX. Este análisis va a evidenciar lo siguiente:

- El estado general y la madurez de las cláusulas o secciones.
- La diferencia entre el estado actual y el ideal en la organización.
- La descripción de las brechas existentes.

Tabla 6. Grado de cumplimiento con la norma ISO/IEC 27001:2013

Cláusulas	% Cumplimiento Actual	Brecha	% Cumplimiento Deseado	Cumplimiento
4. Contexto de la organización	67%	33%	100%	ADMINISTRADO
5. Liderazgo	76%	24%	100%	ADMINISTRADO
6. Planificación	61%	39%	100%	ADMINISTRADO
7. Soporte	72%	28%	100%	ADMINISTRADO
8. Operación	65%	35%	100%	ADMINISTRADO
9. Evaluación del desempeño	52%	48%	100%	DEFINIDO
10. Mejora	45%	55%	100%	DEFINIDO
TOTAL	**63%**	**ADMINISTRADO**		

Fuente: Elaboración propia

De manera gráfica se puede observar que los que tienen el menor porcentaje de cumplimiento son en el eje de Mejora y Evaluación de cumplimiento y el de mayor porcentaje son el eje de Liderazgo y Soporte. ELCATEX debe mejorar de manera significativa cada uno de los ejes para poder lograr el cumplimiento total de cada una de las secciones.

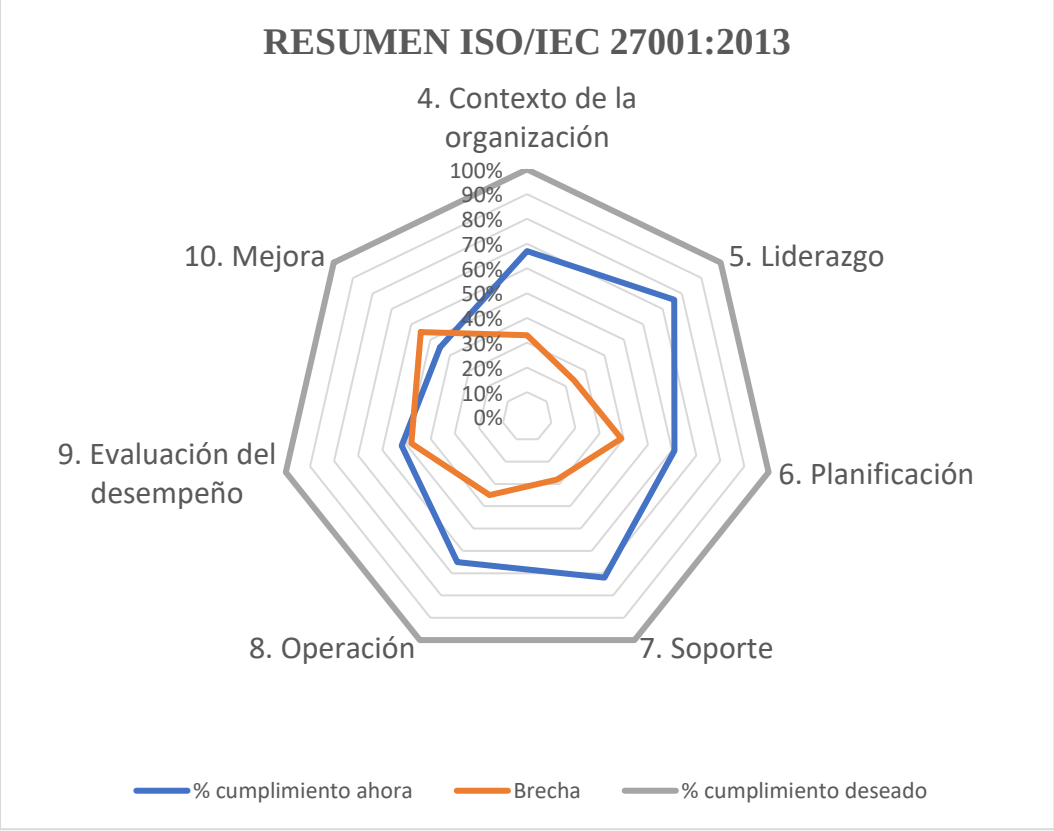


Figura 6: Resumen gráfico de cumplimiento

Fuente: Elaboración Propia

4.2.1 CUMPLIMIENTO NORMATIVO ISO/IEC 27001:2013

4.2.1.1 CONTEXTO EN LA ORGANIZACIÓN

El grado de cumplimiento en la cláusula de ‘Contexto de la organización’ es de 67%, por lo que su brecha es del 33%. Uno de los aspectos positivos en esta dimensión es que la organización ha identificado los objetivos del Sistema de Gestión de Seguridad de la Información y que se ha determinado como las partes internas y externas pueden suponer amenaza para la seguridad de la información, pero en este momento existe una debilidad en cuanto a que no existe en su totalidad o de manera formal un listado de requisitos sobre SGSI referente a reglamentos, requisitos legales y requisitos contractuales.

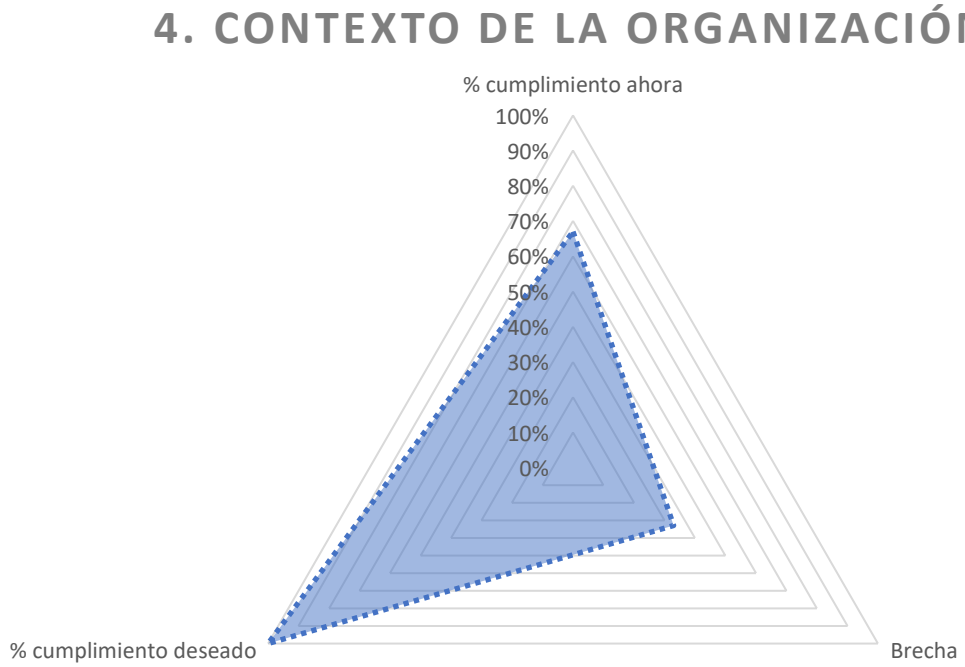


Figura 6 Cumplimiento eje normativo 4

Fuente: Elaboración propia

4.2.1.2 LIDERAZGO

El eje de liderazgo fue evaluado en tres secciones: Liderazgo y compromiso, Política de la Seguridad de información y Roles y Responsabilidades. El grado de cumplimiento en la cláusula de 'Liderazgo es de 76%, por lo que su brecha es del 24%. Este eje es el que mejor desempeño actual tiene. Actualmente en ELCATEX su solidez se centra en el que la dirección provee los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI y que se han asignado las responsabilidades y autoridades sobre la SGSI. Una de las áreas de mejora en la dimensión de "Liderazgo" que se analizó es de que no se mantiene información documentada de la política del SGSI y de sus objetivos.

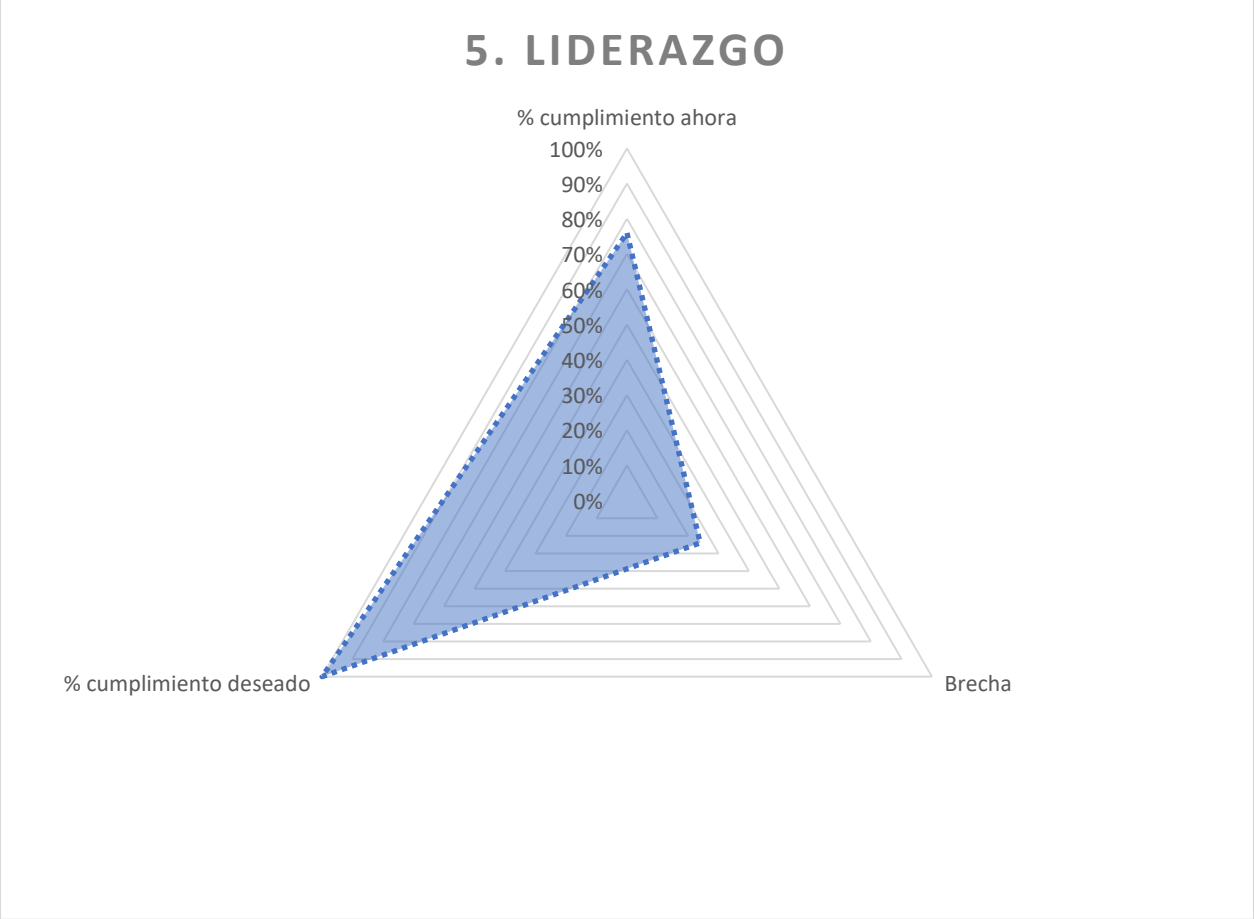


Figura 7. Cumplimiento eje normativo 5

Fuente: Elaboración propia

4.2.1.3 PLANIFICACIÓN

El eje de Planificación fue evaluado en dos secciones: Tratamiento de riesgos y oportunidades y Planificación para consecución de objetivos. El grado de cumplimiento de esta cláusula es de 61%, por lo que su brecha es del 39%. Dentro de la fortaleza que se identificaron en este eje es que se han integrado los objetivos de la Seguridad de la Información en los procesos de la organización y se identificó como una oportunidad de mejora que actualmente en la organización no se ha establecido los criterios para elaborar una declaración de aplicabilidad. Si ELCATEX desea implementar en la norma ISO/IEC 27001:2013 en un futuro, se recomienda poder tener dicho documento ya que este formato es usado previo a la auditoria de certificación.

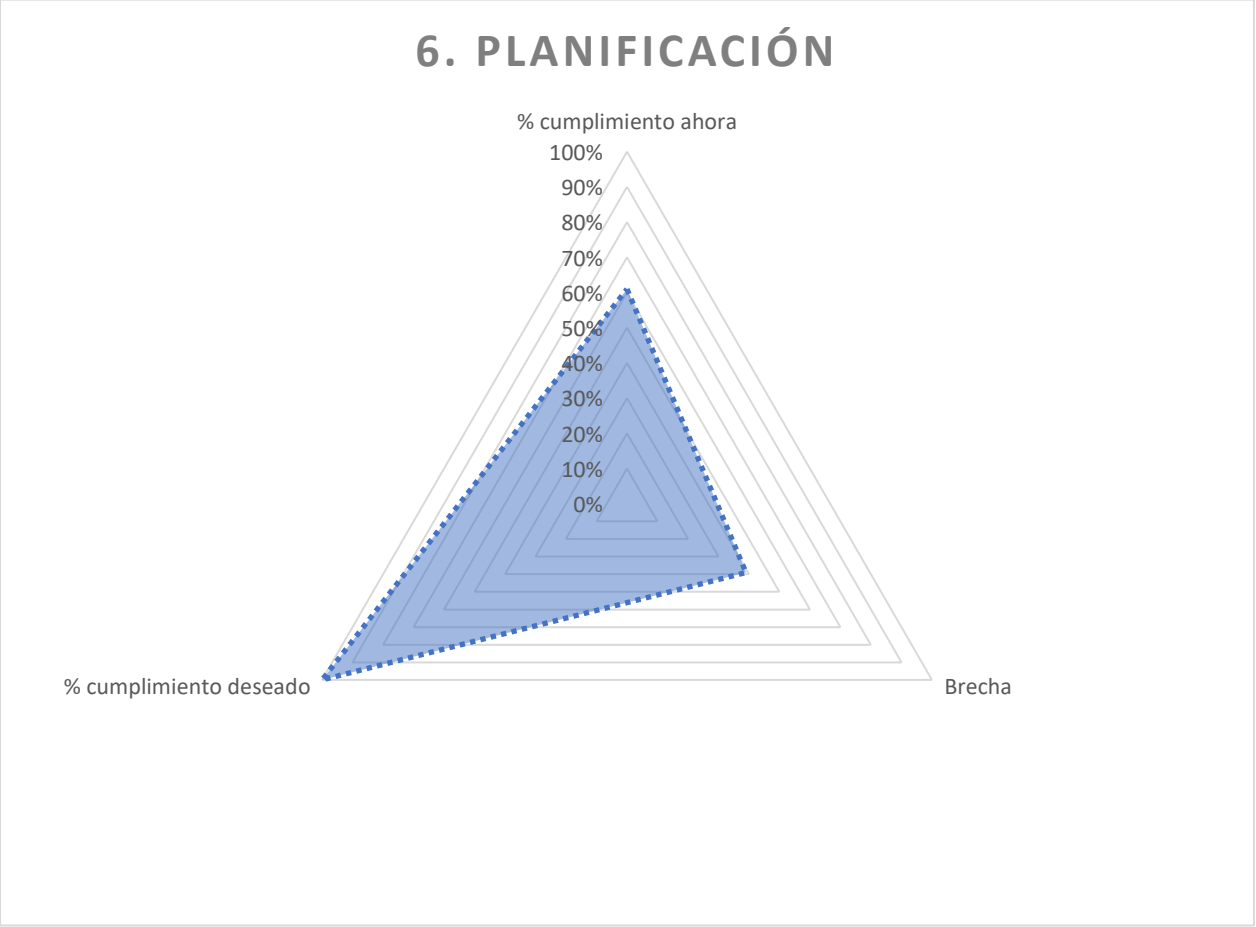


Figura 8 Cumplimiento eje normativo 6

Fuente: Elaboración propia

4.2.1.4 SOPORTE

El eje de Soporte es el segundo mejor evaluado dentro de esta investigación. Actualmente cuenta con 72% de cumplimiento de la cláusula y tiene un 28% de brecha. Dentro de ELCATEX el personal está involucrado y está consciente de su papel en la Seguridad de información y se mantiene la información actualizada sobre la competencia del personal. Dentro de una oportunidad de mejora en este eje se encuentra que no se cuenta con su totalidad de documentos exigidos por la norma ISO/IEC 27001:2013 y que no se dispone en su total los procesos principales de la seguridad de la información.

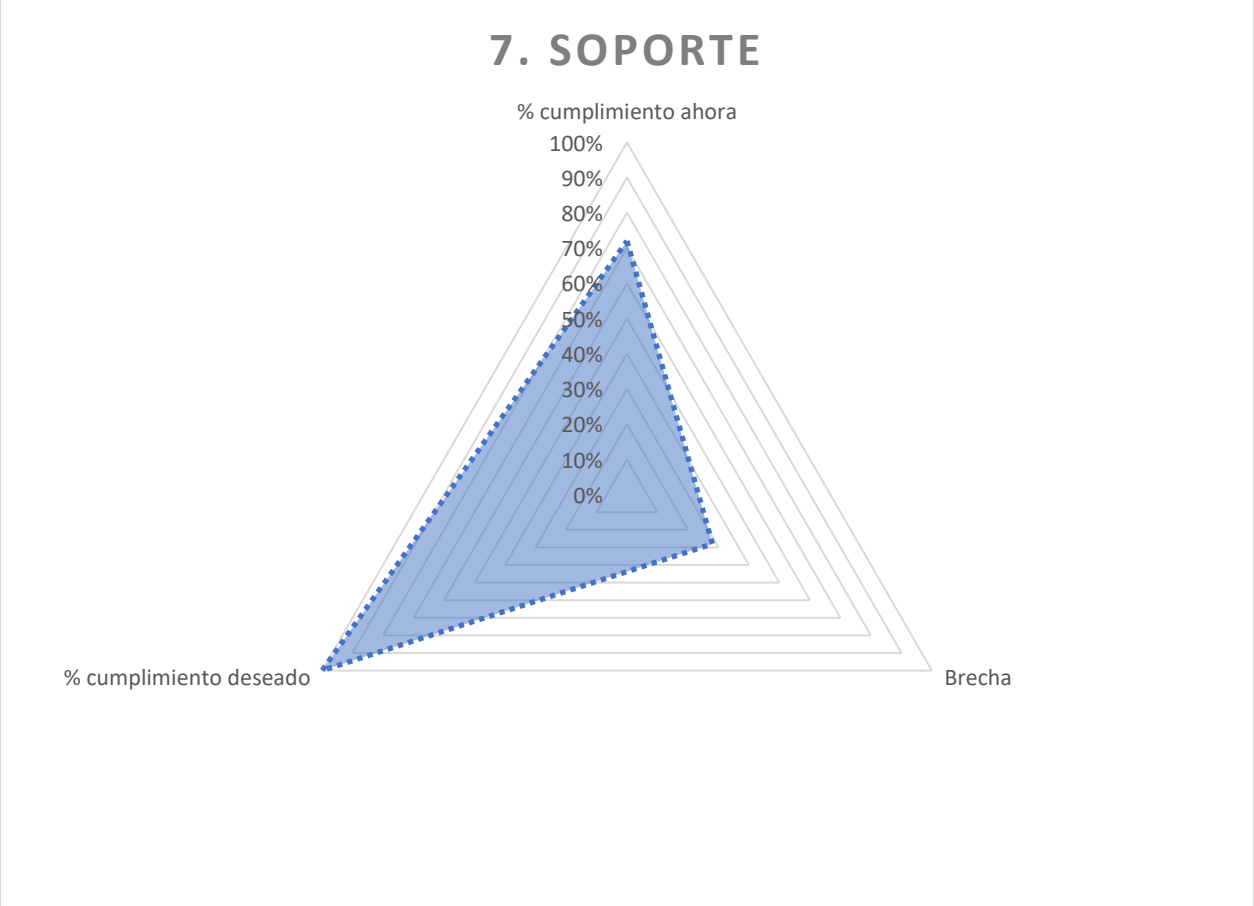


Figura 9 Cumplimiento eje normativo 7

Fuente: Elaboración propia

4.2.1.5 OPERACIÓN

El eje de Operación cuenta con un 65% de cumplimiento y fueron evaluados tres secciones: Control Operacional, Análisis de riesgos de la Seguridad de la Información y Tratamiento de riesgos de la SGSI. Un aspecto positivo en este eje es la identificación y control de los procesos externos en cuanto a los riesgos para la Seguridad de la Información, pero dentro de los aspectos a mejorar en este eje es que no se cuenta actualmente con un análisis y evaluación de riesgos para la Seguridad de información. En dicho documento se tiene que detallar: El propietario del riesgo, la importancia del riesgo o nivel de impacto y la probabilidad de ocurrencia.

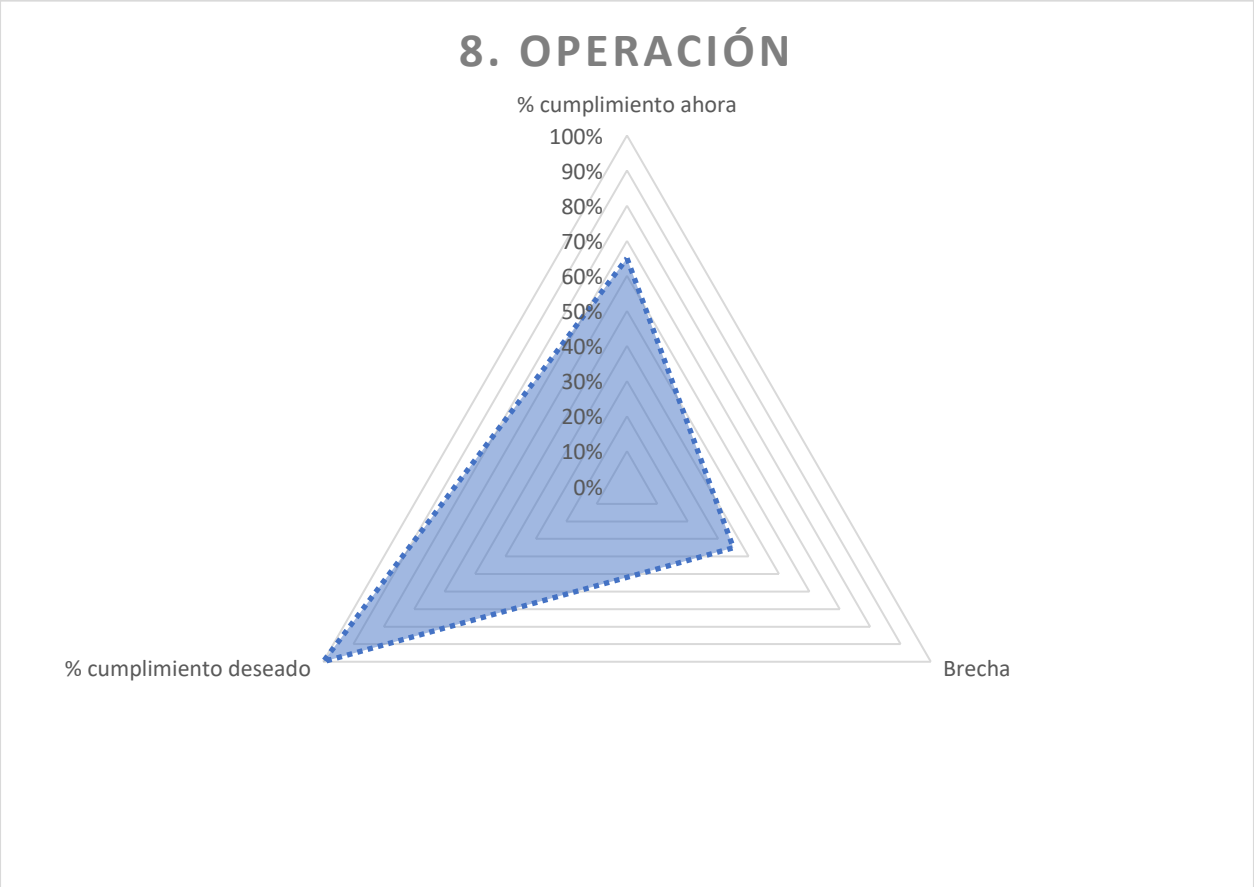


Figura 10 Cumplimiento eje normativo 8

Fuente: Elaboración propia

4.2.1.6 EVALUACIÓN DEL DESEMPEÑO

El eje de "Evaluación del desempeño" cuenta con un 52% de cumplimiento por lo que su nivel de brecha es del 48%. Este eje es uno de los que más se recomienda realizar acciones para poder mejorar el desempeño general dentro de la organización. Tres secciones fueron evaluadas en este eje: Seguimiento y medición, Auditorías Internas e Informe de revisión por Dirección. Dentro de los puntos a mejorar son: No existe una programación para los informes de la dirección y existe constancia de su realización periódica y durante las auditorías internas no se ha definido el alcance y los requisitos para el informe de auditoría. También se recomienda mejorar el proceso de documentar las evaluaciones de los resultados de las mediciones y sobre qué resultados son tomados en cuenta por los responsables tanto de los procesos como de la Seguridad de la Información.

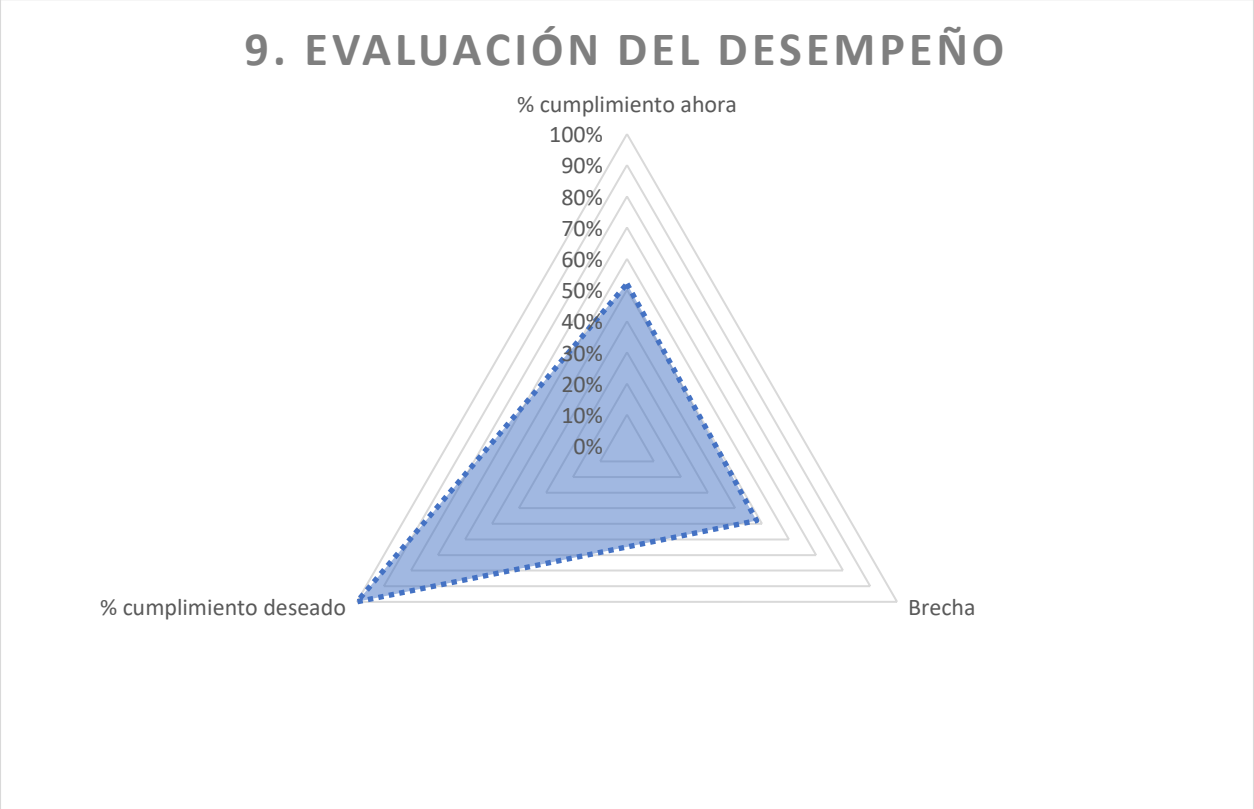


Figura 11 Cumplimiento eje normativo 9

Fuente: Elaboración propia

4.2.1.7 MEJORA

El eje de “Mejora” es el eje que muestra el menor grado de cumplimiento y por el que se recomienda tomar acciones. Actualmente cuenta con 45% de cumplimiento por lo que representa un 55% de brecha. Dos secciones fueron evaluadas en dicho eje: No conformidades y acciones correctivas y Mejora Continua. En este momento, en ELCATEX no cuenta con un proceso que garantice la mejora continua del SGSI identificando las oportunidades de mejora y dentro de las acciones correctivas no existe una diferencia entre acciones correctivas sobre la no conformidad y sobre las causas de esta.

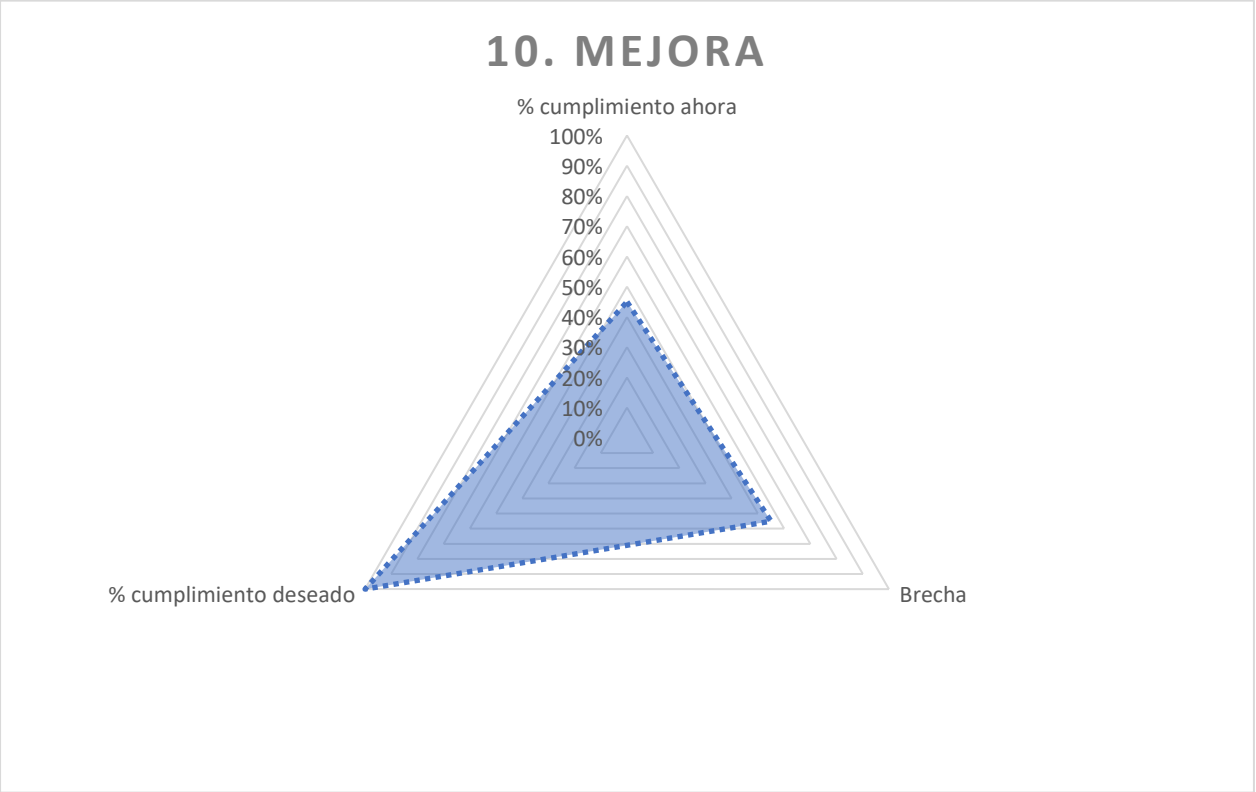


Figura 12 Cumplimiento eje normativo 10

Fuente: Elaboración propia

4.2.2 CUMPLIMIENTO CONTROL ISO/IEC 27001:2013

El anexo A de la norma ISO/IEC 27001:2013 se puede encontrar los catorce controles para poder medir el nivel de madurez y de los cuales se mencionan a continuación y a la misma vez se define los interlocutores por cada sección.

1. A.5 - Políticas de Seguridad de la Información
    - Interlocutor: Dirección + Todos los departamentos.
2. A.6 - Organización de la Seguridad de la Información.
    - Interlocutor: Director Departamento TI
3. A.7- Seguridad en los Recursos Humanos.
    - Interlocutor: Director RRHH
4. A.8 - Gestión de Activos
    - Interlocutor: Director Operaciones y Director de TI
5. A. 9- Control de Acceso
    - Interlocutor: Director Operaciones
6. A.10- Criptografía
    - Interlocutor: Director Operaciones y Director de TI
7. A.11- Seguridad Física y del entorno
    - Interlocutor: Director Operaciones
8. A.12- Seguridad en las Operaciones
    - Interlocutor: Director Operaciones y Director de TI
9. A.13- Seguridad en las Comunicaciones.
    - Interlocutor: Director Operaciones y Director de TI
10. A.14- Adquisición, desarrollo y mantenimiento de sistemas de información. (Interlocutor: director Departamento TI)
    - Interlocutor: Director Departamento TI
11. A.15- Relación con Proveedores
    - Interlocutor: Director RRHH
12. A.16- Gestión de incidentes de seguridad de la información.
    - Interlocutor: Director Departamento TI

13. A.17- Gestión de la Continuidad del Negocio.
    - Interlocutor: Dirección + Todos los departamentos
14. A.18- Cumplimiento
    - Interlocutor: Departamento Legal

Mediante la técnica de la entrevista, se realizó una serie de preguntas a personas, que tienen amplio conocimiento del tema y que son Gerentes/directores del área. Una vez terminada la entrevista se procedió a la evaluación de los datos para conocer el nivel medio cumplimiento. La norma, plantea la siguiente formula:

> Nivel Medio Cumplimiento = Puntuación total de cada control/ Número de controles totales.

La fórmula nos presentará un valor medio para cada control entre 0 y 5, por lo que se podrá clasificar los controles y su cumplimento entre los siguientes valores:

- Puntaje de madurez por debajo de 1.65 - No cumple
- Puntaje de madurez entre 1.66 y 3.25 - Cumple parciamente
- Puntaje de madurez por encima de 3.26 – Cumple con los requisitos de la norma

En el Anexo 10: Encuesta de Cumplimiento de Controles, Anexo A ISO/IEC 27001:2013, se podrá ver con más detalle las 117 preguntas de los controles. Dado que el tipo de respuesta de cada pregunta está en una escala de Likert, se consideró lo siguiente:

- Totalmente de acuerdo será igual a 5
- De acuerdo será igual a 4
- Neutral será igual a 3
- En desacuerdo será igual a 2
- Totalmente de acuerdo será igual a 1

La operación matemática aplicada en este Cumplimento Control es el siguiente:

1. Colocar la respuesta de cada pregunta en el formato.
2. Considerando las respuestas hacer la relación en la escala de 1-5 que se comentó en el párrafo anterior.
3. Hacer una sumatoria de todos en base a la escala de (5,4,3,2,1)
4. Se considerará que:
    a. Totalmente de acuerdo y De acuerdo será igual a “Cumple”
    b. Neutral será igual a “Parcial”
    c. En desacuerdo y Totalmente desacuerdo será igual a “No cumple”
5. Obtener el % de cumplimiento.

En el Anexo 11, se puede encontrar más detalle de los resultados en el Cumplimento Control y a continuación una tabla resumen del porcentaje de cumplimiento de los controles. Como resultado se obtiene que, de manera global, un 64% de los 14 controles de la norma ISO/IEC 27001:2013 se cumplen en ELCATEX y 23% se cumplen de manera ‘parcial’ y un 13% no se cumple.

Tabla 7. Resumen del Porcentaje de Cumplimiento de los Controles de la Norma ISO/IEC 27001:2013.

GRUPO DE CONTROLES		CUMPLE	PARCIAL	NO CUMPLE
Controles Operacionales	A9. Control de Acceso	100%	0%	0%
	A14. Adquisición, desarrollo y mantenimiento de sistemas de información	38%	38%	23%
	A16. Gestión de incidentes de seguridad de la información	0%	29%	71%
	A17. Gestión de la Continuidad del Negocio	58%	33%	8%
	SUBTOTAL	**49%**	**25%**	**26%**
Controles de gestión:	A5. Políticas de Seguridad de la Información	100%	0%	0%
	A6. Organización de la Seguridad de la Información	0%	86%	14%
	A7. Seguridad en los Recursos Humanos	100%	0%	0%
	A15. Relación con Proveedores	0%	40%	60%
	A18. Cumplimiento	88%	13%	0%
	SUBTOTAL	**58%**	**28%**	**15%**
Controles técnicos	A8. Gestión de Activos	80%	20%	0%
	A10. Criptografía	50%	50%	0%
	A11. Seguridad Física y del entorno	100%	0%	0%
	A12. Seguridad en las Operaciones	94%	6%	0%
	A13. Seguridad en las Comunicaciones	93%	7%	0%
	SUBTOTAL	**83%**	**17%**	**0%**
TOTAL		**64%**	**23%**	**13%**

Fuente: Elaboración propia

En la Figura 13: Nivel de Madurez – Controles ISO 27001 muestra el resultado de la entrevista en donde se puede identificar que el A15 (Relación con Proveedores), A16 (Organización de la Seguridad de la Información) no se cumplen y que necesitan apoyo para poder realizar correcciones y poder mejorar el desempeño. Actualmente en ELCATEX no se ha establecido de manera formal y completa requisitos de seguridad de la información en contratos con terceros y no se controla los cumplimientos de los requisitos establecidos con proveedores externos. En la sección de "Organización de la Seguridad de la información" no se tiene definido responsabilidades y procedimientos para responder a los incidentes de la SGSI y no se han implementado canales adecuados para la comunicación de incidentes en la seguridad de la información.

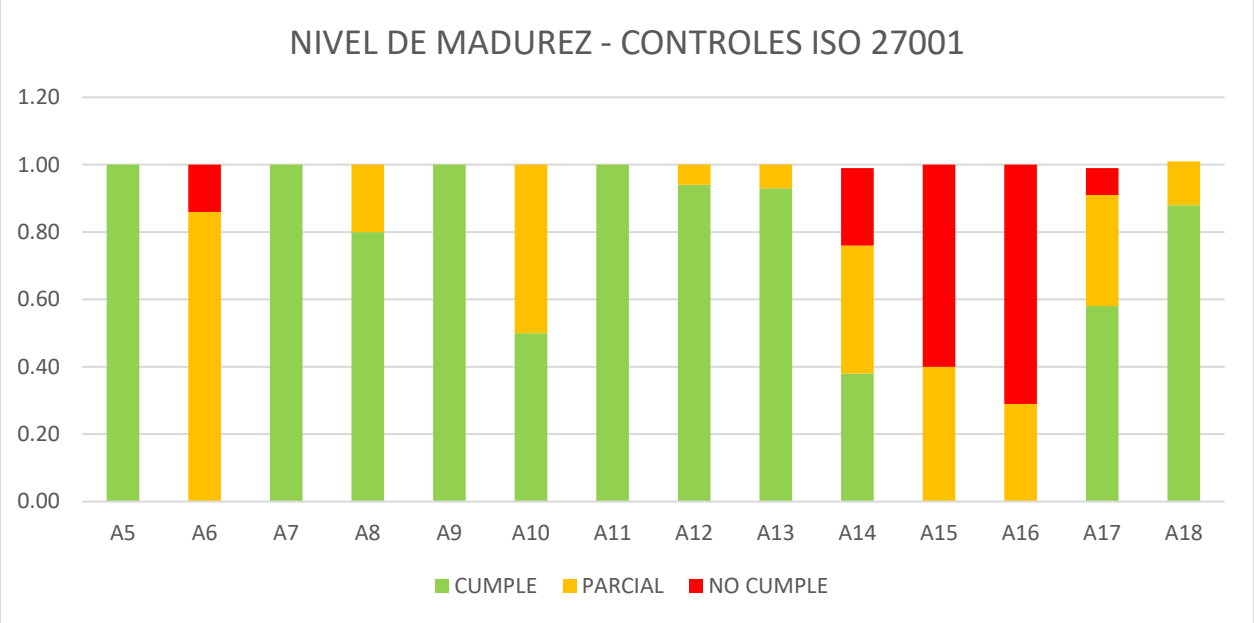


Figura 13. Nivel de Madurez- Controles ISO/IEC 27001:2013

Fuente: Elaboración propia

En una segmentación por las tres categorías de los Controles de la Norma ISO/IEC 27001:2013: Control Operacional, Control de Gestión y Control Técnico se puede observar que el control que tiene mejor desempeño es el Control Técnico, con un porcentaje global de cumplimiento del 83% ya que en ELCATEX protege los equipos tanto del medioambiente como de acceso no autorizados, están establecidos perímetros de seguridad física donde es necesario y

existen sistemas de detección para software malicioso y por último se tiene establecido sistemas de copias de seguridad acordes con la necesidades de la información y de los sistemas.

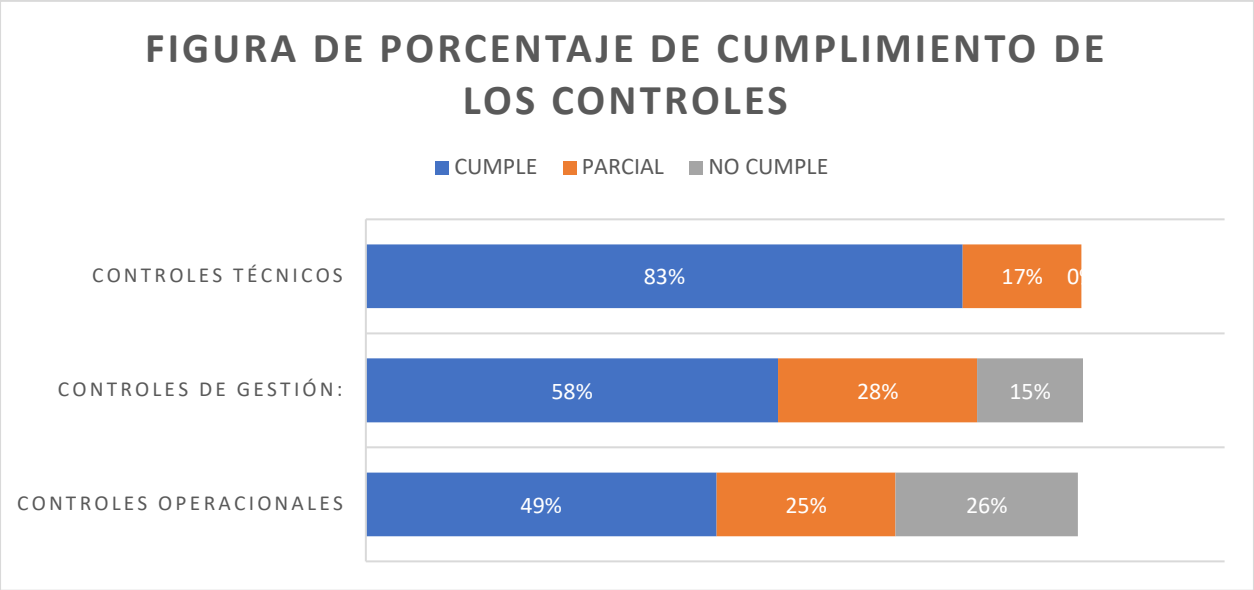


Figura 14. Porcentaje de Cumplimiento de los Controles por Categoría.

Fuente: Elaboración propia

4.3 BENEFICIOS DE LA IMPLEMENTACIÓN PARA ELCATEX DE LA NORMA ISO/IEC 27001:2013

Dentro de los beneficios de la implementación para ELCATEX, se encuentran:

1. Contar con un SGSI como ISO 27001 le permitirá a ELCATEX proteger los datos y prevenir las consecuencias que traería la materialización de un riesgo de este tipo.

2. Lograr que sus colaboradores, cliente y proveedores adopten una cultura de seguridad de la información que les permita minimizar los riegos a perdidas de información o violaciones a sus sistemas de información.

3. Reducir superficie de ataque al asegurar que sus sistemas de información, equipos, sitios de trabajo, y demás activos están siendo utilizados bajos las mejores prácticas que la norma estipula en sus controles de gestión.

4. Contar con procesos documentados, asegurando de esta manera que los métodos utilizados permiten gestionar la confidencialidad, integridad y disponibilidad de la información.

5. Promover la sistematización de esquemas de auditoria periódicas que en apego a los procesos de mejoramiento continuo deben ir de la mano con la evolución y crecimiento natural de la corporación, asegurando que estos puntos no afecten las buenas prácticas del SGSI ya implementadas.

6. El contar con un SGSI implementado le permite a la compañía transmitir confianza a sus aliados estratégicos, clientes y proveedores, garantizándoles que la información que forma parte de los procesos de la cadena de suministro está siendo tratada en cumplimiento de los tres pilares de la seguridad de la información.

7. Implementar el SGSI le permite a la organización contribuir en el cumplimiento de objetivos corporativos y potenciar la imagen corporativa.

8. Asegurar la resiliencia operativa, mediante un plan detallado para enfrentar brechas de seguridad o concretización de amenazas, al tener documentado y sistematizado su plan de recuperación de desastres.

4.4 PRUEBA DE HIPOTÉSIS

Para poder realizar la prueba de hipótesis planteada en la presente investigación es necesario establecer las siguientes condiciones:

a) Si, el valor G_1 es menor o igual a 50%, se acepta H_0

   $G_1 \leq H_0$ se acepta

b) Si, el valor G_1 es mayor a 50%, se rechaza H_0 y se acepta H_i

   $G_1 \geq H_0$ se rechaza H_0

En esta investigación se está analizando toda la población, por lo tanto, el valor de G_1 es igual al 63%, por lo tanto, se cumple la condición b, por lo tanto, se rechaza H_0 y se acepta H_i.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

Una vez analizado los resultados obtenidos mediante la metodología que fue propuesta en esta investigación se procederá a concluir los resultados más significativos y por medio de las recomendaciones se muestran alternativas para guiar a ELCATEX en su proceso de implementación de la norma ISO/IEC 27001:2013.

5.1 CONCLUSIONES

Las conclusiones están basadas en la resolución de las variables propuestas en cada uno de los objetivos planteados y en la hipótesis, por lo que tenemos lo siguiente:

1. En el presente trabajo de investigación se elaboró una evaluación inicial o diagnóstico de la empresa ELCATEX en temas relacionados con Seguridad de la Información y protección de datos basada en la percepción del grupo de interés, en el cual se pudo determinar que el grado de implementación actual es del 63% de cumplimiento de los ítems de la norma ISO/IEC 27001:2013 y que existe un 37% de brecha global.

2. Mediante la utilización de un análisis de brecha, se identificó que aspectos no están en conformidad con la norma ISO/IEC 27001:2013. Se calificó de manera porcentual en base a cien el cumplimiento de cada uno de los ejes normativos siendo el de Liderazgo el que presenta la menor brecha en el cumplimiento y el de Mejora con la mayor brecha de no conformidad.

3. Dentro de los beneficios que puede obtener ELCATEX al momento de implementar la norma ISO/IEC 27001:2013 es: A) Puede proporcionar a la organización una ventaja competitiva ante la competencia (Ejemplo: Hanesbrands y Gildan). Si un cliente también está certificado con la norma ISO 27001, es muy probable que optará por trabajar con proveedores en cuyos controles de seguridad de la información confié. B) Apoya el desarrollo de una cultura interna que está alerta a

los riesgos de la información y por ende la operación del día a día en ELCATEX podría llegar hacer más eficiente ya que reduciría la interrupción del negocio en un determinado momento. C) Provee tranquilidad a propietarios y gerentes en ELCATEX ya que al contar con un SGSI sólido y eficaz pueden estar más serenos que no estarán expuestos a riesgos y que puedan afectar la reputación de la empresa ELCATEX.

4. Se determinó que elementos o pasos debe de contener una guía diseñada para dirigir el proceso de implementación de un sistema de seguridad de la información en ELCATEX. Dichos elementos son: Fase 1- Evaluación Inicial para conocer la brecha en términos de ISO 27001, Fase 2- Determinar el alcance del SGSI en ELCATEX. Fase 3- Elaboración de la política y objetivos del SGSI en ELCATEX. Fase 4- Catalogo y valoración de amenazas para la Seguridad de la Información en ELCATEX. Fase 5- Estructurar los documentos obligatorios del SGSI en ELCATEX. Fase 6- Establecer Indicadores de Procesos. Fase 7- Plan de Comunicación ISO 27001 al personal de ELCATEX Fase 8- Auditorías Internas según ISO 27001 y Fase 9-Revision del SGSI por parte de la dirección.

5.2 RECOMENDACIONES

Para cada una de las variables de estudio y en base a las conclusiones planteadas en el apartado anterior, se recomienda que:

1. Definir de manera estructurada responsables por área y el grado de responsabilidad de cada colaborador, quienes deben asegurar el cumplimiento de los controles y mejores prácticas definidas por el SGSI y que deben ser aplicadas de manera diferenciada para cada grupo de gestión según resultados del análisis de gestión de riesgos, con el apego directo en los procesos de mejoramiento continuo para optimizar su cumplimiento en cada proceso de la Compañía.

2. Establecer los controles de ajuste necesario para reducir la brecha existente entre la situación actual y lo recomendado por el SGSI establecidos en la norma ISO 27001, para garantizar el cumplimiento general en todos sus aspectos, haciendo uso de las plantillas, flujos y procedimientos recomendados por ISO y que reflejen enfoque en lograr los objetivos y estrategia corporativa.

3. Explotar la ventaja competitiva que le brinda a una organización la implementación de un SGSI basado en la norma ISO 27001 que puede ser aprovechado por sus socios estratégicos, clientes y proveedores para el tratamiento de la información generada en las transacciones comerciales y de soporte en la cadena de suministro.

4. Mantener un involucramiento activo de la alta gerencia y todas las partes interesadas de Organización para mantener y dar sostenibilidad a una cultura de seguridad de la información en ELCATEX, haciendo uso de campañas de socialización activas, con contenido y mensajes renovados periódicamente que hagan referencia a los controles de la norma y resaltar la importancia de los activos.

5. Establecer la sistematización de auditoría periódicas sobre los procesos y validación de cumplimiento del SGSI con generación de informes dirigidos a los responsables de velar por el cumplimiento de los controles.

6. Seguir utilizando marcos de referencia para el manejo efectivo de sus procesos de gestión tanto en servicios de tecnología como flujos operativos y potenciarlos realizando benchmarking para la identificación de oportunidades de mejora y así promover la optimización de estos.

CAPÍTULO VI. APLICABILIDAD

En este capítulo se lleva a cabo el diseño de la guía para la implementación de un sistema de gestión de la información. Los resultados obtenidos en los capítulos anteriores; serán la base para conocer cada uno de los elementos o acciones que debe contener la guía.

6. 1 NOMBRE DE LA PROPUESTA

Guía para la implementación de un SGSI para el Aseguramiento de la Cadena de Suministro en ELCATEX.

6.2 JUSTIFICACIÓN DE LA PROPUESTA

La importancia de contar con un SGSI sólido y confiable, se enfoca en garantizar la seguridad en el tratamiento de datos para la empresa ELCATEX de modo que se reduzcan las posibilidades de la pérdida de información y que por ende no sea afectada la cadena de suministro. La aplicación correcta del documento actual posibilita un mayor aprendizaje en los directivos quienes son los encargados de implementar las políticas de seguridad informática, cuyos conocimientos obtenidos facilitarían el desarrollo de nuevos modelos de gestión que se encaminen hacia la mejora del funcionamiento organizacional.

Luego de aplicar la encuesta de “Test de cumplimiento de ISO/IEC 27001:2013” se obtuvo el resultado que todos los ejes normativos no están en total cumplimiento con dicha norma y que los ejes que muestran mayor brecha son el eje de Mejora y Evaluación de desempeño, por lo que se propone una guía para poder mejorar en estos puntos.

6.3 ALCANCE DE LA PROPUESTA

La guía es aplicable para lograr el cumplimiento de conformidad con los requisitos detallados en la norma de sistemas de gestión de seguridad de la información ISO/IEC 27001:2013 para ELCATEX y tiene como objetivos:

a) Plantear un procedimiento para poder realizar un análisis de riesgo en la organización basado en un sistema de gestión de seguridad de la información.

b) Establecer los controles normativos que deben ser implementados para reducir la brecha actual y lo definido con la norma ISO/IEC 27001:2013 y así elaborar una guía personalizada para la empresa ELCATEX en base a dicha norma.

6.4 DESCRIPCIÓN Y DESARROLLO A DETALLE DE LA PROPUESTA

Los elementos de la guía propuesta fueron basados en los lineamientos de la misma norma ISO/IEC 27001:2013 adaptado a ELCATEX.

6.4.1 ESTRUCTURA Y COMPOSICIÓN DE LA GUÍA

La guía propuesta consta de dos secciones, detalladas de la siguiente manera:

a) Sección primera: Contiene el procedimiento para poder realizar un análisis de riesgo en ELCATEX ya que esto va a permitir reducir el riesgo operacional a través de la implementación de políticas de seguridad sobre los riegos identificados. Al realizar un análisis de riesgo resultará fundamental en determinar los niveles de probabilidad y severidad de los diversos niveles de amenazas.

b) Sección segunda: Contiene las herramientas y los recursos necesarios que le permitirán a ELCATEX cumplir con cada uno de los debes o aspectos mandatorios con los cuales actualmente no está en conformidad según lo detallado en la norma de requisitos para los sistemas de gestión de la información ISO/IEC 27001:2013 para poder lograr la satisfacción del cliente y optimizar sus procesos.

Las fases en dicha guía son los siguientes:

1. Fase 1: Auditoria Inicial ISO 27001 en ELCATEX
2. Fase 2: Análisis del contexto de la organización
3. Fase 3: Elaboración de la política y objetivos del SGSI
4. Fase 4: Planificación del SGSI
5. Fase 5: Documentación del SGSI
6. Fase 6: Implementando el SGSI
7. Fase 7: Comunicación y sensibilización SGSI
8. Fase 8: Auditoría interna según ISO 27001
9. Fase 9: Revisión por la dirección según ISO 27001
10. Fase 10: El proceso de certificación ISO 27001

6.4.2 ELEMENTOS Y ACTIVIDADES DE LA GUÍA POR SECCION

A continuación, se detallan por sección; cada uno de los elementos que debe ejecutar la empresa ELCATEX para poder cumplir con un análisis de riesgo e identificar los pasos necesarios para poder implementar ISO/IEC 27001:2013 en ELCATEX. Como lo plantea (ISO 27001) estos tienen su base documental y estructural según lo dicta la norma.

A) Sección primera: Elementos relacionados para poder realizar un análisis de riesgo en ELCATEX.

1. Al realizar un análisis de riesgo es fundamental determinar los niveles de probabilidad y severidad obteniendo así los diversos niveles de amenazas como son muy alto, moderado y bajo, es por ello por lo que la calificación de cada uno de los riesgos del modelo de gestión está dada de acuerdo con la siguiente tabla:

Tabla 8- Matriz de Riesgo Propuesto

Factor de Riesgo		Severidad		
		Mínima (4)	**Media (6)**	**Crítica (8)**
Probabilidad	**Poco Probable (3)**	Bajo (12)	Bajo (18)	Moderado (24)
	Probable (5)	Bajo (20)	Moderado (30)	Alto (40)
	Muy probable (9)	Moderado (36)	Alto (54)	Muy alto (72)

Elaboración: Propia

Para obtener la evaluación de cada riesgo, se sigue la siguiente formula: Probabilidad x Severidad = Evaluación del riesgo.

2. Luego de haber evaluado el riesgo, es posible establecer las posibles consecuencias de cada una de ellas, estableciendo así una calificación de acuerdo con sus niveles de probabilidad y severidad para de esta manera obtener sus categorías de riesgos y en base a ello identificar los correspondientes tipos de políticas que son necesarias implementar en un Sistema de Gestión de Seguridad de la Información. La siguiente tabla puede servir como base para un futuro análisis:

Tabla 9 – Riesgos identificados y políticas de seguridad Propuesto

Factor de Riesgo	Descripción	Probabilidad	Severidad	Evaluación del riesgo	Nivel de riesgo	Políticas de Seguridad
Riesgo de reputación	Virus maliciosos en programas informáticos	5	8	40	Alto	Política de software no autorizado

Elaboración: Propia

3. Una vez se obtenga un análisis completo de riesgo es recomendable contar con la revisión por parte de los directivos de ELCATEX al menos una vez al año, con el propósito de que se pueda asegurar el cumplimiento adecuado.

B) Sección segunda: Pasos, herramientas y los recursos necesarios que le permitirán a ELCATEX cumplir con cada uno de los debes o aspectos mandatorios y requisitos para la adopción e implementación del sistema de gestión de la seguridad de la información ISO/IEC 27001:2013. La guía propuesta está basada en la propia norma ISO 27001 y la mayoría del texto en esta sección ha sido adoptada del sitio web www.Normaiso27001.es que explica en detalle la norma y ofrece además recomendaciones generales para su implementación.

1. Fase 1- Auditoria Inicial ISO 27001 GAP y Fase 2 Análisis del contexto de la Organización

Las primeras fases fueron previamente analizadas y se encuentran en el documento presente.

2. Fase 3- Elaboración de la política y objetivos del SGSI.

2.1 Política de Seguridad.

La situación actual en ELCATEX es que el 79% está de acuerdo que se ha establecido los objetivos del SGSI y que el 64% establece que si está definido las Políticas de Seguridad. Por lo tanto, se recomienda que la política debe de indicar como mínimo lo siguiente y publicarlo una vez esté terminado para que todos los involucrados estén al tanto.

Se recomienda considerar los siguientes aspectos al momento de la elaboración de la Política de Seguridad:

1. Redactar una política de acuerdo con las necesidades de ELCATEX

2. La política de la seguridad de la información debe tener en cuenta los objetivos corporativos de ELCATEX.
3. La política del SGSI debe demostrar que se tienen en cuenta los requisitos de las partes interesadas.
4. La comunicación de la política a las partes interesadas.
5. Se debe definir el propietario de la política.

Elementos de la Política de Seguridad que ELCATEX debe de incluir:

- El alcance del SGSI
- Las responsabilidades del SGSI
- La estructura de la empresa
- Metodología para el análisis y evaluación de riesgos.

Para desarrollar la política de seguridad en ELCATEX, se sugiere definir los objetivos en base a las siguientes categorías:

- Protección de activos de información
- Autenticación
- Autorización
- Integridad de la información

3. Fase 4- Planificación del SGSI

Dentro de la Fase 4 está el análisis del riesgo y su Plan de Tratamiento el cuál fue expuesto en la sección primera.

4. Fase 5- Documentación del SGSI

La situación actual en ELCATEX es que el 36% de los Gerentes afirman que ELCATEX no ha establecido criterios para elaborar una declaración de

aplicabilidad y que un 43% comentan que los documentos de origen externo no se controlan, por lo tanto, se propone contar con los siguientes documentos obligatorios del SGSI, según lo afirma (ISO 27001):

1. El alcance del SGSI
2. Política de seguridad de la información
3. Proceso de evaluación de riesgos de seguridad de la información
4. Proceso de tratamiento de riesgos de seguridad de la información
5. La declaración de aplicabilidad
6. Objetivos de seguridad de la información
7. Información documentada determinada por la organización como necesaria para la efectividad del SGSI
8. Planificación y control operacional
9. Resultados de la evaluación de riesgos de SGSI
10. Resultados del tratamiento de riesgo de SGSI
11. Evidencia del monitoreo y medición de resultados
12. Un proceso de auditoría interna documentado
13. Evidencia de los programas de auditoría y los resultados de la auditoría
14. Evidencia de la naturaleza de las no conformidades y cualquier acción posterior tomada

Entre los documentos específicos que nos solicita el Anexo A de la norma ISO 27001 se encuentra lo siguiente y se sugiere a ELCATEX tenerlos presente:

1. Definición de funciones y responsabilidades de seguridad (A 7.1.2 y A.13.2.4).
2. Un inventario de activos (A 8.1.1).
3. Reglas para el uso aceptable de los activos (A 8.1.3).
4. Esquema de clasificación de la información (A.8.2.1).
5. Política de control de acceso (A.9.1.1).

6. Procedimientos de operación para la administración de TI (A 12.1.1).
7. Registros de actividades del usuario, excepciones y eventos de seguridad (A 12.4.1 y A.12.4.3).
8. Principios de ingeniería de sistemas seguros (A 14.2.5).
9. Política de seguridad del proveedor (A 15.1.1).
10. Procedimiento de gestión de incidentes (A 16.1.5).
11. Procedimientos de continuidad del negocio (A 17.1.2).
12. Requisitos legales, reglamentarios y contractuales (A 18.1.1).

5. FASE 6- Implementación de un SGSI

Actualmente en ELCATEX es que el 36% de los Gerentes y Directores afirman que el sistema de Gestión de Seguridad de la Información no está establecido o implementado y que el 50% manifiesta que no se ha implementado un plan de tratamiento de riesgos en donde los propietarios del riesgo estén informados y han aprobado un plan de control.

Por lo que se sugiere seguir los siguientes elementos para poder mejorar la puntuación en este aspecto. Según lo comenta (ISO 27001), en este punto se deben definir los procesos de seguridad e integrarlos a los procesos del negocio, tomando en cuenta los hallazgos reconocidos y los controles para aminorar los riesgos para llegar a mantener los niveles tolerables en la información en ELCATEX.

Es indispensable la asignación de tareas y responsabilidades al personal de ELCATEX para desarrollar un plan de tratamiento de riesgos y la implementación de los controles y procesos de seguridad, ellos deberán realizar las siguientes tareas sugeridas:

- Establecer los objetivos de las medidas de seguridad.
- Hacer efectivas las medidas organizativas.

- Implementar y ejecutar las tareas técnicas planificadas.
- Supervisar las actividades.
- Recabar y analizar la información de los indicadores.

5.1 Estableciendo indicadores de procesos

Una vez que los directores en ELCATEX hayan definido los procesos, se recomienda establecer indicadores ya que estos van a medir el cumplimiento o no de dichos elementos. Los elementos mínimos necesarios para determinar los indicadores son los siguientes:

- Descripción del control.
- Criterios de medición.
- Valores indicativos.
- Forma de cálculo para evaluar resultados
- Periodicidad/frecuencia de las medidas

5.2 Implementación del proceso

Al superar cada uno de estos puntos ELCATEX podrá argumentar que ha pasado la primera fase de implementación.

6. Fase 7- Comunicación y sensibilización SGSI

En este momento un 64% de los Directores y Gerentes en ELCATEX sostiene que el personal está involucrado y está consciente en su papel en la Seguridad de la Información y un 57% afirma que existe una conciencia del personal sobre los daños que pueden producir el no seguir las pautas de la Seguridad de la Información.

Por lo que se sugiere seguir los siguientes elementos para poder mejorar la puntuación en este aspecto. Según lo comenta (ISO 27001) el Plan de Comunicación debe de dar respuesta a los siguientes puntos

- ¿Quién debe comunicar los aspectos de seguridad?
- ¿A quiénes debe llegar la comunicación?
- ¿Cuál es el contenido?
- ¿En qué momento ha de realizarse la comunicación?
- ¿Qué medios se utilizarán?

Se recomienda un plan de comunicación interno bien diseñado y aplicado de manera efectiva que permita comunicar a toda la organización de la postura de seguridad de la información que ELCATEX está adoptando, como también hacer ver:

- Por qué es necesario el SGSI en ELCATEX.
- Cuáles son las responsabilidades legales de la organización.
- Cómo afectara a cada empleado y área de la empresa cuando el programa esté implantado.

6.1 Documentación del plan de comunicación del SGSI

Se debe preparar una estrategia para un plan de comunicación donde se reflejen los objetivos de la implementación para cada área y se pueda medir el grado de involucramiento de cada responsable en el establecimiento de lo que podremos llamar cultura de la seguridad en ELCATEX.

6.2 Crear la cultura de la seguridad

Se recomienda crear un comité responsable de brindar el acompañamiento al proceso de creación de la cultura de seguridad de la información, comunicación de los

principios y valores de ELCATEX para promover la adopción de la cultura de seguridad, para lo cual se debe:

- Establecer la ruta para las acciones en favor de la seguridad de la información.
- Definir los principios rectores o procedimientos que se consideren necesarios para la seguridad de la información.
- Transmitir a los empleados las expectativas de la dirección sobre cómo deben actuar.

6.3 Educando al personal

Se debe identificar a los empleados que pueden convertirse en agentes de cambio para fortalecer el proceso de implementación del sistema de gestión de seguridad de la información, es importante que estos estén debidamente capacitados para realizar estas tareas de la manera correcta. No se trata de que todo el personal obtenga un certificado formal de estar capacitado en los temas de seguridad de la información, sino de conseguir que todos actúen según la postura de seguridad planteada por la dirección para que la información de ELCATEX esté debidamente protegida.

Como tareas de apoyo a esta etapa de la implementación se recomienda:

- Establecer un programa continuo de concientización sobre la seguridad de la información para garantizar la capacitación inicial, actualizaciones y recordatorios periódicos.
- Los empleados no necesitan saber todo sobre la seguridad de la información, pero se deben concentrar los esfuerzos en que los empleados conozcan los riesgos del trabajo que desempeñan y cómo minimizarlos.
- Las descripciones de los procesos y los fallos en la seguridad de la información revelados en las auditorías internas o externas también se deben

utilizar como material de apoyo al planificar la capacitación de los empleados.

- Las presentaciones en PowerPoint o cualquier medio usado, deben centrarse en ejemplos prácticos en lugar de enumerar cosas que los empleados no pueden hacer.

6.4 Evaluar el cumplimiento

El factor humano representa la mayor amenaza para la seguridad de la información en todas las empresas, por lo tanto, en ELCATEX se debe establecer un método de retroalimentación sobre el nivel en que los empleados están cumpliendo con los principios de la política de la seguridad de la información y las directrices giradas en torno a ello. Por esta razón cada empleado debe conocer cuáles son las ventajas y desventajas de cumplir con las normas de seguridad de la información.

Se recomienda presentar a cada empleado las consecuencias de una actuación poco segura y el por qué vale la pena invertir tiempo en el cumplimiento de la seguridad de la información y los beneficios que obtendremos.

7- Fase 8- Auditoría interna según ISO 27001

En la actualidad el 43% de los Directores y Gerentes en ELCATEX afirman que se ha establecido una programación de auditorías internas y se ha asignado responsables y que el 36% testifica que se han definido los alcances y los requisitos para el informe de auditoría.

Según lo comenta (ISO 27001) y para poder mejorar en este aspecto en ELCATEX, se debe sugiere establecer un plan de auditorías internas que permita revisar el sistema de gestión de seguridad de la información que con ello se pretende:

- Cerciorar que el SGSI que se ha implementado cumple con los requisitos de la norma.
- Inspeccionar que lo necesario en los procesos de ELCATEX se ha incorporado correctamente en los controles de la seguridad de la información seleccionados del SGSI.

7.1 Con la auditoría del SGSI se busca obtener los siguientes beneficios:

- Preparar a ELCATEX para la auditoria de certificación tolerando la identificación y corregir cualquier problema antes de que se lleve a cabo.
- Distinguir pertinencias de mejora.
- Generar evidencia que el SGSI se está revisando continuamente.

7.2 Es importante acotar las tareas de responsabilidad del Auditor del SGSI.

- Realización de informes.
- Conocer y preparar la certificación.
- Monitoreo permanente del cumplimiento del SGSI.

7.3 Definición del equipo de auditores

Se recomienda designar un auditor por cada departamento como lo son Recursos Humanos, Finanzas, Compras, TI y cada una de las áreas o departamentos de ELCATEX. El nombramiento de auditores internos por departamentos aumenta la responsabilidad y reduce el riesgo de errores que podrían surgir por la falta de recursos incidiendo también en el control y seguimiento de las acciones preventivas y correctivas.

Sabiendo que ELCATEX cuenta con un departamento de Auditoría Interna se puede utilizar sus competencias profesionales para establecer el esquema de auditoría de procesos del SGSI y que estos a su vez puedan capacitar a los empleados que deben participar

activamente en cada área tomando tareas de auditor del SGSI apoyando el proceso como agente de cambio.

7.4 Recomendaciones para tener en cuenta al realizar la auditoría internamente:

- Dedicar al proceso el tiempo necesario para la validación de los controles seleccionados del Anexo A, reservar el tiempo requerido es crucial para el proceso de auditoria en cada departamento.

- Delegar o segmentar las tareas de auditoría entre distintos auditores, por lo que se sugiere aprovechar las habilidades, puntos fuertes y experiencia de cada auditor.

7.5 Evaluar o auditar la comprensión de los objetivos del SGSI y su cumplimiento.

Se debe validar en qué grado los empleados comprenden la importancia de la seguridad de la información por lo que se recomienda el uso de evaluaciones periódicas con calificación mínima de aprobado.

7.6 Soporte para mejorar el sistema SGSI

Es importante tener reuniones con los responsables de los diferentes departamentos y compartir los hallazgos, discutir las dudas que se presenten y acordar las oportunidades de mejora para poder presentar un informe que sirva para la mejora continua del sistema.

8 Fase 9- Revisión por la dirección según ISO 27001

Actualmente un 29% de los Directores y Gerentes afirman que no existe una programación para los informes de la dirección y no existe constancia de su realización periódica. Según lo afirma (ISO 27001), lo siguiente son los elementos necesarios en la

fase#9 de la implementación de la norma y sus lineamientos generales y adaptados a la organización son el siguiente:

.

- Objetivo de la revisión por la dirección de ELCATEX:

    - Hay que asegurar que el SGSI y sus objetivos permanezcan siendo adecuados y competente para ELCATEX para alcanzar dicha meta.
    - Verificar la autenticidad de los riesgos identificados que ELCATEX este enfrentando al momento de cada revisión.

- La revisión de la dirección como parte de la mejora continua:

    - Es necesario incorporar el ciclo PDCA también denominado ciclo de Deming, esto como parte de la implementación del SGSI en ELCATEX.

8.1 El ciclo PDCA en la estructura de la norma ISO 27001

Con base en las cuatro fases del conocido ciclo de mejora continua PDCA podemos establecer una correlación con la estructura de la norma ISO 27001.

La etapa de Planificar (PLAN) se toma en cuenta en las primeras cuatro fases de la norma, de esta manera se genera una correspondencia directa entre la planificación del sistema y los capítulos cuatro, cinco, seis y siete de la norma ISO 27001:2013.

La etapa de Hacer (DO) se corresponde con la puesta en marcha e implementación del sistema generando la documentación necesaria, implementando los controles para la seguridad de la información que hemos determinado mediante el análisis de riesgos y estableciendo los roles y responsabilidades para las tareas de la seguridad de la información, esta forma parte de la fase cinco, seis y siete del

sistema de gestión, estas fases se corresponden básicamente con el capítulo ocho, de la norma ISO 27001:2013

La etapa de Monitorizar (CHECK) corresponde con los requisitos de la norma enfocados a la evaluación del desempeño del sistema de gestión de la seguridad de la información, tiene su equivalencia en el capítulo nueve de la norma, el cual tiene su desarrolla en las fases ocho y nueve de la implementación del sistema SGSI.

En cuanto la etapa de Actuar (Act), requiere de acciones para la mejora continua del sistema de gestión con base en los hallazgos de la etapa previa, no es suficiente con detectar los incumplimientos o deficiencias del sistema, sino que es necesario establecer un proceso de acciones correctivas sobre los fallos detectados. La norma establece requisitos para esta etapa en el capítulo diez, donde trata básicamente el tema de las acciones correctivas.

8.2 Consideraciones en una revisión del SGSI

Para la revisión del SGSI por parte de la dirección es necesario considerar los siguientes requisitos:

- La revisión de la gestión de ISO 27001 debe incluir al menos:
    - El estado de las acciones de revisiones de gestión anteriores.
    - Cambios en problemas externos e internos que son relevantes para el sistema de gestión de la seguridad de la información.
    - Retroalimentación sobre el desempeño de la seguridad de la información.
    - Los resultados de la evaluación de riesgos y el estado del plan de tratamiento de riesgos.

6.4.3 INDICADORES DE DESEMPEÑO DE LA GUÍA

Para poder medir el grado de avance en el cumplimiento del Sistema de Gestión de Seguridad de la Información es necesario definir indicadores eficaces, con la intención de poder medir todo aquello que brinde soporte al sistema de gestión. Al momento de definirlos se deben tener en cuenta los siguientes aspectos:

- No se deben crear demasiados indicadores, solamente los estrictamente requeridos.
- Los indicadores deben estar alineados con el SGSI, se busca crear soporte para la mejora continua.
- Los indicadores deben agrupar procesos considerados de alta importancia o críticos.
- Los indicadores deben mostrar información en tiempo real.
- Los indicadores deben medir la eficacia, eficiencia, efectividad, calidad, oportunidades de mejora en la ejecución de los controles.

Entre los primeros indicadores que se pueden utilizar se recomiendan los siguientes:

a) Porcentaje de Implementación de Controles.
   - Objetivo: Buscar identificar el grado de avance en la implementación de controles de seguridad en ELCATEX.
   - Tipo de Indicador: Indicador de Gestión y Unidad de medición: Porcentual
   - Variables: X es el número controles implementados y Z es el número total de controles que se planearon implementar.
   - Formula: (X/Z) *100
   - Rango:
     - Mínima (75-80%),
     - Satisfactoria (81-99%)
     - Sobresaliente (100%)

b) Grado de conformidad en SGSI > 63%

c) Grado de cumplimiento de los controles > 64%

6.5 CRONOGRAMA DE IMPLEMENTACIÓN

Se define plan de trabajo basado en 21 semanas para el proceso de implementación, enlistando actividades macro y sus responsables:

Tabla 10- Cronograma de actividades

Feriado

Actividades	Responsable	SEMANA																				
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Inicio																						
Contratación de personal requerido	Gestión de Talento Humano																					
Inducción, Gestión de mobiliario/herramientas de trabajo para personal auditoria	Gestión de Talento Humano / TI																					
Gestión de contratación consultores	Compras / TI																					
Capacitación del personal / auditores	Consultores /TI																					
Elaboración de cronograma de actividades de Planeación del SGSI de ELCATEX	TI / Consultores																					
Presentación/Autorización del Cronograma de Trabajo del SGSI a ELCATEX	TI / Alta Gerencia																					
Campaña de socialización general	Alta Dirección / Desarrollo Organizacional / Gestión de Talento Humano																					
Sección primera - Análisis de riesgo en la organización	Alta Dirección/Dueños de proceso																					
Fase 4: Planificación del SGSI	Alta Dirección/Dueños de proceso																					
Consolidado y etiquetado de Activos de la información	Alta Dirección/Dueños de proceso																					
Identificación de amenazas y vulnerabilidades a partir de la criticidad de los activos de la información	Alta Dirección / Dueños de proceso																					
Definir metodología de valoración de riesgos. Preparar la declaración de aplicabilidad. Preparar Plan de Tratamiento de Riesgos	Alta Dirección / Dueños de proceso																					
Configuración y alimentación de software de control de SGSI / ISO Tools	TI / Consultores																					
Sección segunda - Definición de los controles normativos																						
Fase 3: Elaboración de la política y objetivos del SGSI	Alta Dirección																					
Definición de Roles y Responsabilidades de la norma ISO 27001	Alta Dirección																					
Fase 5: Documentación del SGSI	Alta Dirección / Dueños de proceso																					
Fase 6: Implementando el SGSI	Alta Dirección / Dueños de proceso																					
Fase 7: Comunicación y sensibilización SGSI	Alta Dirección / Desarrollo Organizacional																					
Fase 8: Auditoría interna según ISO 27001	Alta Dirección / Consultores / Auditores																					
Fase 9: Revisión por la dirección según ISO 27001	Alta Dirección																					
Fin																						

Fuente: Elaboración propia

6.6 PRESUPUESTO

Los valores detallados en el siguiente presupuesto carecen de cotizaciones formales para los productos y servicios considerados; sin embargo, se tomó la opinión y valorizaciones de expertos en el tema, así como también los valores detallados en páginas web de empresas nacionales:

Tabla 11- Presupuesto

DESCRIPCION	DETALLE	CANTIDAD	VALOR US$ $	TOTAL
Recurso Humano x (3 personas) - contratacion	Personal contratado para soporte internos de las areas en el proceso de implementacion, documentacion	3	$ 1,000.00	$ 3,000.00
Formación o Capacitación del personal - consultor externo	Capacitacion del personal en la norma ISO 27001	1	$ 2,500.00	$ 2,500.00
Campaña de socializacion	Diseno, material de apoyo y socializacion	1	$ 1,200.00	$ 1,200.00
Tiempo Horas / Hombre - Personal Interno	Factor de tiempo invertido por el personal en actividades propias de la implementacion	1000	$ 5.00	$ 5,000.00
Herramientas Hardware / Software	Computadoras, telefonos, impresoras y licencias de herramientas de software asignadas al equipo de implementacion	1	$ 2,700.00	$ 2,700.00
Software de Gestion ISO Tools - Licencia	Herramienta espacializada para la gestion de documentos, manejo de riesgos, SoA, indicadores	1	$ 5,000.00	$ 5,000.00
Costos de Materiales	Costeo de papeleria, mobiliario y espacios fisicos para personal de Implementacion	1	$ 1,800.00	$ 1,800.00
Consultores Expertos ISO 27001 - Contrato Servicio	Personal de apoyo para la capacitacion del personal, acompanamiento e implementacion del SGSI	2	$ 3,200.00	$ 6,400.00
			$ 17,405.00	**$ 27,600.00**

Fuente: Elaboración propia

6.7 TABLA DE CONCORDANCIA DE LOS SEGMENTOS DE LA TESIS CON LA PROPUESTA.

Con el propósito de mostrar una congruencia entre el trabajo de investigación desarrollado en los capítulos anteriores de este informe y la idoneidad de la propuesta o la aplicabilidad de esta, se presenta la siguiente tabla de concordancia.

Tabla 12- Tabla de Concordancia

Capítulo I			Capítulo II	Capítulo III			Capítulo V	Capítulo VI	
Título Investigación	Objetivo General	Objetivos Específicos	Teorías / Metodologías de sustento	Variables	Poblaciones	Técnicas	Conclusiones	Nombre de la propuesta	Objetivos de la propuesta
Análisis del sistema de información en ELCATEX según norma ISO 27001:2013	Diseñar una guía para la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2013 para el aseguramiento de la cadena de suministro de la empresa ELCATEX	1) Elaborar una evaluación inicial o diagnóstico en temas relacionados con Seguridad de la Información y protección de datos en base a la percepción de Gerentes y Directores evaluados en ELCATEX.	Normalización	Grado de conformidad con la norma ISO/IEC 27001:2013	Alta Gerencia en ELCATEX Gerentes /Directores	Análisis de brecha / Encuesta / Entrevistas	Se determinó que el grado de implementación actual es del 63% de cumplimiento de los ítems de la norma ISO/IEC 27001:2013 y que existe un 37% de brecha global.	Guía para la implementación de un SGSI para el Aseguramiento de la Cadena de Suministro en ELCATEX	1) Plantear un procedimiento para poder realizar un análisis de riesgo en la organización basado en un sistema de gestión de seguridad de la información.
		2) Identificar los aspectos normativos que no están en conformidad con las mejores prácticas de la norma ISO/IEC 27001:2013 en base a la percepción de Gerentes y Directores evaluados en ELCATEX.					Mediante un análisis de brecha, se identificaron los aspectos que no están en conformidad con la norma ISO/IEC 27001:2013. Siendo el control de Mejora y Liderazgo los de mayor brecha de no conformidad.		
		3) Establecer los beneficios que la empresa ELCATEX recibirá al implementar las mejores prácticas de la norma ISO/IEC 27001:2013.		Modelo de madurez de un SGSI			Dentro de los beneficios que puede obtener ELCATEX con la implementación de ISO/IEC 27001:2013 están: adquirir una ventaja competitiva ante la competencia y un apoya permanente al desarrollo de una cultura de seguridad.		2) Establecer los controles normativos que deben ser implementados para reducir la brecha actual y lo definido con la norma ISO/IEC 27001:2013 y así elaborar una guía personalizada para la empresa ELCATEX en base a dicha norma.
		4) Elaborar una propuesta para una Guía de Mejores Prácticas en la seguridad de la información y protección de datos basado en la norma ISO/IEC 27001:2013					Se determinó que elementos o pasos debe contener una guía diseñada para dirigir el proceso de implementación de un sistema de gestión de seguridad de la información en ELCATEX.		

Fuente: Elaboración propia

BIBLIOGRAFÍA

Aguilar Antonio, J. (21 de Abril de 2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. doi:https://doi.org/10.5354/0719-3769.2021.57067

Alonso, L. (1994). *Métodos y técnicas cualitativas de investigación en ciencias sociales.* Madrid.

Arias, G. (1998). *Mitos y errores en la elaboración de Tesis y proyectos de investigación.* Episteme.

Arroyo Guardeño, D., Gayoso Martínez, V., & Hernández Encinas, L. (2020). *Ciberseguridad.* Editorial CSIC Consejo Superior de Investigaciones Científicas.

Avetta Marketing. (19 de Febrero de 2021). Obtenido de https://www.avetta.com/es/blog/encontrar-y-resolver-problemas-de-seguridad-en-la-logistica

Batista, F., Hirtzer, M., & Dorning, M. (2 de Junio de 2021). *Y ahora... ¿nos quedaremos sin carne? Mayor productora del mundo cierra sus plantas tras hackeo*. Obtenido de EL FINANCIERO: https://www.elfinanciero.com.mx/empresas/2021/06/01/y-ahora-nos-quedaremos-sin-carne-mayor-productora-del-mundo-cierra-sus-plantas-tras-hackeo/

Bernal, C. (2016). *Metología de la Investigación: Administración, economía, humanidades y ciencias sociales.* Pearson Educación.

Bonde, A., & Bruno, J. (28 de Enero de 2019). *Forrester*. Obtenido de https://www.forrester.com/report/US-B2B-eCommerce-Will-Hit-18-Trillion-By-2023/RES136173

Cabezas, Y. (31 de Mayo de 2022). *Hackean sistemas de la CCSS durante la madrugada*. Obtenido de CRHOY: https://www.crhoy.com/nacionales/hackean-sistemas-de-la-ccss-durante-la-madrugada/

Campos Cortés, J. (13 de julio de 2007). *Seguridad física y de la información en la cadena de suministro*. Obtenido de Gestiopolis: https://www.gestiopolis.com/seguridad-fisica-y-de-la-informacion-en-la-cadena-de-suministro/

Christensen, L. (1980). *Experimental Methodology* (Ninth Edition ed.). United States of America: Pearson.

CriptoSavia. (12 de Junio de 2021). *CriptoSavia.* Obtenido de McDonald's informó un ciberataque en sus operaciones de Taiwán y Corea del Sur: https://criptosavia.com/mcdonalds-informo-un-ciberataque-en-sus-operaciones-de-taiwan-y-corea-del-sur/

Daruma. (16 de abril de 2016). *El ranking de los países con mayor número de certificados*. Obtenido de Darumasoftware: https://www.darumasoftware.com/gestion-calidad/el-ranking-de-los-paises-con-mayor-numero-de-certificados/

Demeestere, M. (3 de Febrero de 2022). Ataque cibernético contra tres terminales petroleras europeas.

Díaz, R. (2021). *Estado de la ciberseguridad en la logística de América Latina y el Caribe.* Santiago: Comisión Económica para América Latina y el Caribe (CEPAL). Obtenido de https://repositorio.cepal.org/bitstream/handle/11362/47240/1/S2100485_es.pdf

EFE. (9 de Junio de 2021). *El peor ataque cibernético contra EE.UU. lo provocó una contraseña antigua*. Obtenido de EFE: https://www.efe.com/efe/america/economia/el-peor-ataque-cibernetico-contra-ee-uu-lo-provoco-una-contrasena-antigua/20000011-4558298

EFE. (1 de Marzo de 2022). Un ciberataque paraliza la producción de Toyota en Japón durante un día. *EFE*.

EFE News Service. (9 de Mayo de 2022). El 60 % de los ataques cibernéticos a empresas son por "mala configuración".

El Espectador. (29 de Agosto de 2016). En América Latina hay 12 ataques cibernéticos por segundo. Obtenido de https://www.proquest.com/newspapers/en-américa-latina-hay-12-ataques-cibernéticos-por/docview/1814759163/se-2?accountid=35325

ELCATEX. (2020). *Alineamiento Estrategico 2020.* Choloma: ELCATEX.

Escoto, F., & Jipsion, A. (2021). Modelo de observatorio TIC para Honduras.

Forbes Staff. (30 de Abril de 2022). *Forbes Mexico*. Obtenido de Costa Rica sufre ciberataque que paraliza aduanas y sitios web para pago de impuestos: https://www.forbes.com.mx/costa-rica-sufre-ciberataque-que-paraliza-aduanas-y-sitios-web-para-pago-de-impuestos/

García, E. (10 de Junio de 2018). *El Español.* Obtenido de El primer hackeo fue hace 184 años, cuando ni siquiera existían los ordenadores: https://www.elespanol.com/omicrono/software/20180610/primer-hackeo-hace-anos-siquiera-existian-ordenadores/313969318_0.html

Gómez Fernández, L., & Fernández Rivero, P. P. (2018). *Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad.* AENOR.

Gómez, V. (2017). *La Lucha Contra el Ciberterrorismo y los ataques infórmaticos* .

Gonzales, G. (2019). Fuentes primarias: características y ejemplos. Obtenido de https://www.lifeder.com/fuentes-primarias/#:~:text=Las%20fuentes%20primarias%20son%20documentos,sido%20editad

González, H. (25 de Agosto de 2016). GAP ANALISIS PARA IMPLEMENTACIÓN DE ISO.

Grupo Fraga. (2018). *GRUPO FRAGA*. Obtenido de 6 pasos para realizar el análisis de brechas según la ISO 27001: https://grupo-fraga.com/6-pasos-para-realizar-el-analisis-de-brechas-segun-la-iso-27001/

Gutiérrez, L. (2021). *Guía para la implementación de un sistema de Gestión de Calidad y Buenas Prácticas de Manufactura en la Fábrica de Pastas De San Pedro Sula.* UNITEC.

Hernández Sampieri, R., Baptista, & Fernández. (2010). Metodologia de la investigacion. McGraw-Hill.

Hernández Sampieri, R., Collado, C., & Baptista, P. (2014). *Metodología de la investigación.* McGraw Hill Education.

Hernández, L. (30 de Octubre de 2019). Ley de ciberseguridad de Honduras es ambigua y se enmarca en el odio. *Criterio HN*.

Hurtado, M. (2011). *GESTIÓN DE RIESGO METODOLOGÍAS OCTAVE y MAGERIT*. Universidad Piloto de Colombia. Obtenido de http://polux.unipiloto.edu.co:8080/00004420.pdf

IPANDETEC Centroamérica. (2018). *Paso a paso para una política de ciberseguridad integral HONDURAS.*

ISO27000.ES. (2005). *SGSI*. Obtenido de iso27000.es: https://www.iso27000.es/sgsi.html

Jiménez, J. (31 de Diciembre de 2021). *Estos han sido los peores ataques de 2021*. Obtenido de RZ Redes Zone: https://www.redeszone.net/noticias/seguridad/peores-ataques-informaticos-2021/

Jiménez, M. (03 de Diciembre de 2020). Así puedes hacer una matriz de riesgos para tu empresa. Obtenido de https://www.piranirisk.com/es/blog/asi-puedes-hacer-una-matriz-de-riesgos-para-tu-empresa

Krajewski, L. (2013). *Administración de operaciones (10th Edición).* Pearson.

Krauss, C. (11 de Mayo de 2021). *Ciberataque al oleoducto Colonial Pipeline: esto sabemos*. Obtenido de The New York Times: https://www.nytimes.com/es/2021/05/11/espanol/colonial-pipeline-ransomware.html

León, M. (22 de septiembre de 2020). *Estadística de las Normas ISO más Implementadas a Nivel Mundial*. Obtenido de R & D Consulting: https://www.rd.com.pa/2020/09/22/estadistica-de-las-normas-iso-mas-implementadas-a-nivel-mundial/

Martín, E. (21 de Julio de 2020). ¿Qué es la ciberseguridad? Obtenido de https://www.grupocibernos.com/blog/que-es-la-ciberseguridad

Moisés, V. (2014). *Implementación efectiva de un SGSI.*

Molina, S., & Quintero, J. (2022). *DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA EMPRESA BONOS Y DESCUENTOS S.A.S, A PARTIR DE LA NORMA ISO 27001:2013.* Bogota.

Morales Rojas, J. (30 de Marzo de 2022). Influencia del COVID 19 en el incremento de los Ciberataques a Nivel Mundial. Universidad Piloto de Colombia. Obtenido de http://repository.unipiloto.edu.co/handle/20.500.12277/11574

NCSI. (2019). National Cyber Security Index. (E.-G. Academy, Ed.) Obtenido de https://ncsi.ega.ee/

normaiso27001.es. (s.f.). *ISO 27001*. Obtenido de normaiso27001.es: https://normaiso27001.es/

O'Neill , P. (16 de Noviembre de 2020). El ciberataque ransomware no causó la muerte de la paciente alemana. *Opinno*. Obtenido de https://www.technologyreview.es/s/12853/el-ciberataque-ransomware-no-causo-la-muerte-de-la-paciente-alemana

Parrado, V. (2020). *¿Qué es la declaración de aplicabilidad, SOA? y ¿Cuál es su utilidad?*

Pino, R. (2010). *Metodología de la Investigación.* Editorial San Marco,.

Población García, F. J. (2013). *La gestión del riesgo en empresas industriales.* Delta Publicaciones.

Raudales, C. (2017). *La brecha existente en la ciberseguridad en Honduras.* Innovare.

Rigler, E. (1987). *Focus on focus groups.* ABA .

Rios. (2004). *Auditando con matrices de riesgo.* Buenos Aires.

Rivas-Tovar, L. (2015). ¿Como hacer una Tesis ? México. doi:10.13140/RG.2.1.3891.5281

RPP. (3 de Agosto de 2021). Una serie de ciberataques detuvo la vacunación contra la COVID-19 en Italia. *RPP*. Obtenido de https://rpp.pe/tecnologia/mas-tecnologia/una-serie-de-ciberataques-detuvo-la-vacunacion-contra-la-covid-19-en-italia-noticia-1350699?ref=rpp

Ruiz, A. (2019). *PLAN DE GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN.*

SOPHOS. (2022). *El estado del ransomware 2022.* Obtenido de https://news.sophos.com/es-es/2022/06/09/el-estado-del-ransomware-en-el-sector-sanitario-2022/#:~:text=State%20of%20Ransomware%20in%20Healthcare%202022&text=El%20estudio%20revela%20una%20creciente,m%C3%A1s%20amplio%20para%20este%20sector

Soto, A. (2018). *Variables, dimensiones e indicadores en una tesis.*

Tamayo, M., & Tamayo. (2003). El proceso de la investigación científica. LIMUSA.

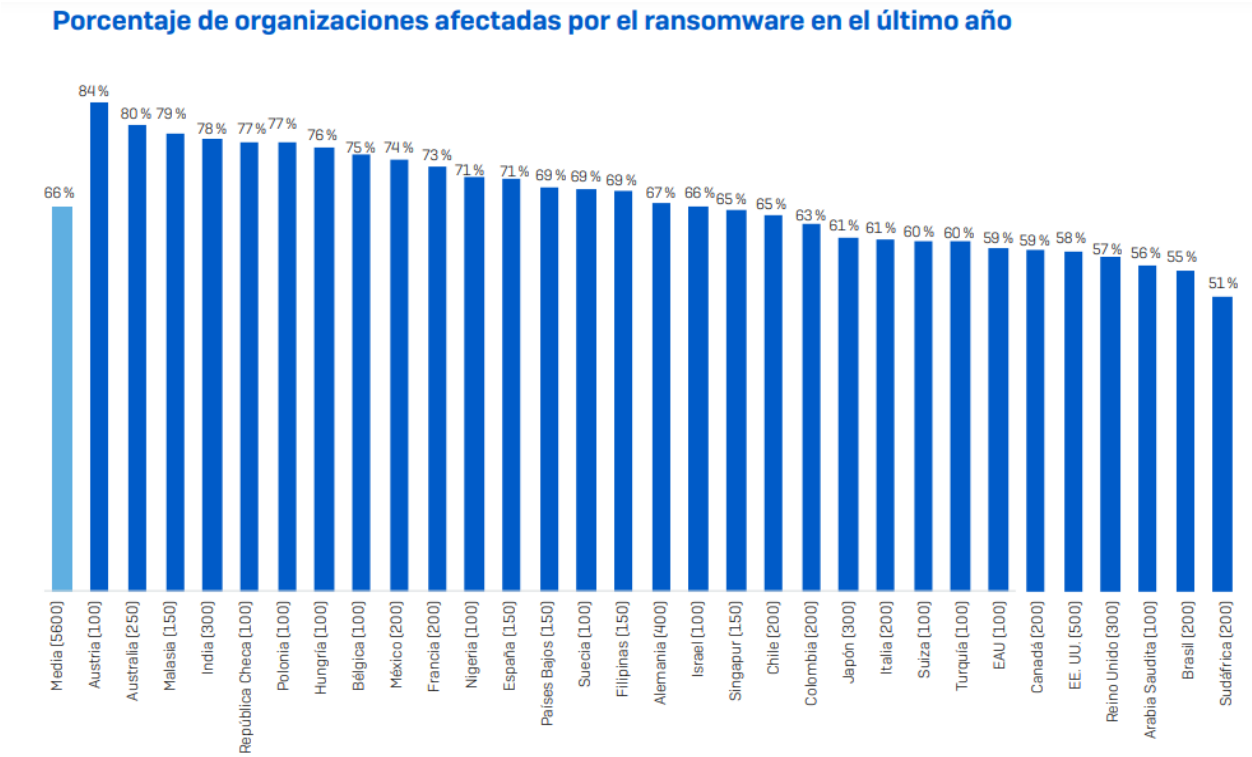
TELENOR. (s.f.). *Política de la seguridad de la información*. Obtenido de telenorcomunicaciones.com: https://telenorcomunicaciones.com/es/politica-si

Terrado, A. A. (2007). *La cadena de suministro.* El Cid Editor.

Tola, D. (2015). *Implementanción de un Sistema de Gestión de Seguridad de la Información para una empresa de consultoria y auditorií, aplicando la norma ISO/IEC 27001.* Guayaquil.

Zelaya, O. (23 de abril de 2021). *HONDURAS – La protección de datos en Honduras*. Obtenido de Central Law: https://central-law.com/honduras-la-proteccion-de-datos-en-honduras/

ANEXO 3. PORCENTAJE DE ORGANIZACIONES AFECTADAS POR RANSOMWARE



ANEXO 4. BALANCE SCORE CARD

Visión:	Ser la organizacion de manufactura textil referente a nivel mundial			
Misión:	Liderar una cultura de mejora continua a través de procesos, productos y servicios innovadores que maximicen el valor para nuestros clientes asegurando la sostenibilidad y desarrollo integral de nuestros colaboradores.			
Áreas de Enfoque:	**Crecimiento de Negocio**	**Innovación**	**Excelencia Operacional**	**Equipo de Excelencia**
Resultado Estratégico:	Aumentar ventas, reducir costos, mejorar la rentabilidad y la liquidez	Atender las exigencias del mercado y estableciendo la nueva forma de operar.	Generar valor con calidad excepcional, mayor eficiencia, mejor tiempo de repuesta, menor costo y maxima flexibilidad	Ser un equipo capaz, con alto sentido de pertenencia y responsable por su entorno

Objetivos Estratégicos	Indicadores	Metas 2021	2022	2023	2024	2025	Iniciativas 2021
Financiera	Indice de Rentabilidad	5.37%	5.93%	6.54%	7.04%	7.47%	
	Variación de Ventas	12%	15%	15%	15%	18%	
	Costo por Libra	-5.0%	-12.7%	-11.6%	-9.1%	-6.0%	
	Costo por Minuto	-6.5%	-2.5%	-1.0%	-1.0%	-1.6%	
Cliente	Adherencia Actual a lo Programado	90%	93%	95%	98%	100%	•Programa de Benchmarking
	# de Regiones Nuevas	0	1	1	1	1	•Sistema de retroalimentación de consumidor y Cliente
	Cantidad de Desarrollos Fullpackage	571	708	831	892	900	•Sistema de Gestión de desarrollo de productos (PDM)
							•Programa de Alianzas Estratégicas
Procesos Internos	Libras por Empleado Directo	2388	2581.85	2912.89	2912.89	3413.02	•Programa de Innovación
	Docenas Por empleado Directo	67.84	68.94	69.65	70.37	71.48	•Sistema de Calidad en la Fuente
	Tasa de Labor indirecta Textil	35.4%	32.8%	30.2%	27.6%	25.0%	•Sistema Solución de Problemas
	Tasa de Labor indirecta Costura	17.0%	16.0%	15.0%	14.0%	14.0%	•Sistema de Trabajo Estándar
	% Bueno a la Primera Vez	80.6%	83.6%	87.1%	90.6%	93.0%	•Mantenimiento Productivo Total
	Cantidad de Iniciativas de Innovación	500	550	600	650	700	•Implementación de NOW
	Tiempo de Entrega (Semanas)	12	11	8	6	4	•Programa de control de Proveedores
							•Programa Gestión Logística
							•Gobierno de Datos y BI
Capacidad Organizacional	# De Horas Promedio de Entrenamiento	18	20	22	25	25	•Programa de Capacitación
	Plantas con reconocimiento Shingo	0	0	2	2	3	•Programa de Recompensa Total
	Accidentes Reportados	25	17	12	6	0	•Programa ADN Corporativo
	Incidentes Registrados	75	51	36	18	2	•Programa de Sostenibilidad
	Cumplimiento Higg Index	100%	100%	100%	100%	100%	•Sistema de comunicación
	Cantidad de Iniciativas de Tecnologia	29	35	41	47	53	•Sistema de Seguridad (EHS)
Principios:	•Construir Confianza •Observar y Resolver •Enfoque en el Proceso •Flujo y Velocidad de Respuesta •Búsqueda de la Perfección •Calidad en la Fuente •Alineamiento Estratégico •Crear Valor para el Cliente						

ANEXO 7. ANÁLISIS DE CONFIABILIDAD DE PRUEBA PILOTO

Item Statistics

	Mean	Std. Deviation	N
1	.67	.577	3
5	.33	.577	3
6	.67	.577	3
8	.67	.577	3
15	.67	.577	3
17	.67	.577	3
18	.67	.577	3
19	.67	.577	3
20	.67	.577	3
22	.33	.577	3
26	.33	.577	3
30	.33	.577	3
32	.67	.577	3
33	.67	.577	3
36	.67	.577	3
37	.67	.577	3
39	.33	.577	3
43	.67	.577	3
46	.33	.577	3

Inter-Item Correlation Matrix

	1	5	6	8	15	17	18	19	20	22	26	30	32	33	36	37	39	43	46
1	1.000	.500	-.500	-.500	-.500	1.000	1.000	1.000	1.000	.500	.500	.500	1.000	1.000	-.500	1.000	.500	1.000	-1.000
5	.500	1.000	.500	-1.000	-1.000	.500	.500	.500	.500	-.500	-.500	1.000	.500	.500	-1.000	.500	-.500	.500	-.500
6	-.500	.500	1.000	-.500	-.500	-.500	-.500	-.500	-.500	-1.000	-1.000	.500	-.500	-.500	-.500	-.500	-1.000	-.500	.500
8	-.500	-1.000	-.500	1.000	1.000	-.500	-.500	-.500	-.500	.500	.500	-1.000	-.500	-.500	1.000	-.500	.500	-.500	.500
15	-.500	-1.000	-.500	1.000	1.000	-.500	-.500	-.500	-.500	.500	.500	-1.000	-.500	-.500	1.000	-.500	.500	-.500	.500
17	1.000	.500	-.500	-.500	-.500	1.000	1.000	1.000	1.000	.500	.500	.500	1.000	1.000	-.500	1.000	.500	1.000	-1.000
18	1.000	.500	-.500	-.500	-.500	1.000	1.000	1.000	1.000	.500	.500	.500	1.000	1.000	-.500	1.000	.500	1.000	-1.000
19	1.000	.500	-.500	-.500	-.500	1.000	1.000	1.000	1.000	.500	.500	.500	1.000	1.000	-.500	1.000	.500	1.000	-1.000
20	1.000	.500	-.500	-.500	-.500	1.000	1.000	1.000	1.000	.500	.500	.500	1.000	1.000	-.500	1.000	.500	1.000	-1.000
22	.500	-.500	-1.000	.500	.500	.500	.500	.500	.500	1.000	1.000	-.500	.500	.500	.500	.500	1.000	.500	-.500
26	.500	-.500	-1.000	.500	.500	.500	.500	.500	.500	1.000	1.000	-.500	.500	.500	.500	.500	1.000	.500	-.500
30	.500	1.000	.500	-1.000	-1.000	.500	.500	.500	.500	-.500	-.500	1.000	.500	.500	-1.000	.500	-.500	.500	-.500
32	1.000	.500	-.500	-.500	-.500	1.000	1.000	1.000	1.000	.500	.500	.500	1.000	1.000	-.500	1.000	.500	1.000	-1.000
33	1.000	.500	-.500	-.500	-.500	1.000	1.000	1.000	1.000	.500	.500	.500	1.000	1.000	-.500	1.000	.500	1.000	-1.000
36	-.500	-1.000	-.500	1.000	1.000	-.500	-.500	-.500	-.500	.500	.500	-1.000	-.500	-.500	1.000	-.500	.500	-.500	.500
37	1.000	.500	-.500	-.500	-.500	1.000	1.000	1.000	1.000	.500	.500	.500	1.000	1.000	-.500	1.000	.500	1.000	-1.000
39	.500	-.500	-1.000	.500	.500	.500	.500	.500	.500	1.000	1.000	-.500	.500	.500	.500	.500	1.000	.500	-.500
43	1.000	.500	-.500	-.500	-.500	1.000	1.000	1.000	1.000	.500	.500	.500	1.000	1.000	-.500	1.000	.500	1.000	-1.000
46	-1.000	-.500	.500	.500	.500	-1.000	-1.000	-1.000	-1.000	-.500	-.500	-.500	-1.000	-1.000	.500	-1.000	-.500	-1.000	1.000

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
1	10.00	21.000	.945	.	.756
5	10.33	25.333	.115	.	.808
6	10.00	31.000	-.778	.	.854
8	10.00	28.000	-.327	.	.832
15	10.00	28.000	-.327	.	.832
17	10.00	21.000	.945	.	.756
18	10.00	21.000	.945	.	.756
19	10.00	21.000	.945	.	.756
20	10.00	21.000	.945	.	.756
22	10.33	22.333	.672	.	.774
26	10.33	22.333	.672	.	.774
30	10.33	25.333	.115	.	.808
32	10.00	21.000	.945	.	.756
33	10.00	21.000	.945	.	.756
36	10.00	28.000	-.327	.	.832
37	10.00	21.000	.945	.	.756
39	10.33	22.333	.672	.	.774
43	10.00	21.000	.945	.	.756
46	10.33	32.333	-.965	.	.862

Resumen de procesamiento de casos

		N	%
Casos	Válido	3	100,0
	Excluido[a]	0	,0
	Total	3	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,802	,802	19

ANEXO 8. ENCUESTA DE CUMPLIMIENTO DE NORMA ISO/IEC 27001:2013

4	La Organización y su Contexto	SI	NO
4.1	**Entendiendo la Organización y su contexto**		
1.-	¿Están identificados los objetivos del SGS Sistema de Gestión de la Seguridad de la Información?		
2.-	¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?		
3.-	¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información?		
4.2	**Expectativas de las partes interesadas**		
1.-	¿Se han identificado las partes interesadas?		
2.-	¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?		
3.-	¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?		
4.3	**Alcance del SGSI**		
1.-	¿Se ha determinado el alcance del SGS y se conserva información documentada?		
4.4	**SGS Sistema de Gestión de la Seguridad de la información**		
1.-	¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?		
5	**Liderazgo**		
5.1	**Liderazgo y compromiso**		
1.-	¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio?		
2.-	¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?		
3.-	¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?		
5.2	**Política de la Seguridad de la Información**		
1.-	¿Se ha definido una Política de la Seguridad de la Información?		
2.-	¿Se ha establecido un marco que permita el establecimiento de objetivos?		
3.-	¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda la empresa?		
4.-	¿Se mantiene información documentada de la política del SGSI y de sus objetivos?		
5.3	**Roles y Responsabilidades**		
1.-	¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información?		
2.-	¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información?		

6	Planificación	SI	NO
6.1	**Tratamiento de Riesgos y Oportunidades**		
1.-	¿El plan para abordar riesgos y oportunidades considera las expectativas de las partes interesadas en relación a la Seguridad de la Información?		
2.-	¿Se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos?		
3.-	¿Se ha definido un proceso de tratamiento de riesgos?		
4.-	¿Se han establecido criterios para elaborar una declaración de aplicabilidad?		
5.-	¿Se mantiene información documentada de los puntos anteriores?		
6.2	**Planificación para consecución de objetivos**		
1.-	¿Se han establecido objetivos de la Seguridad de la Información medibles y acordes a los objetivos del negocio?		
2.-	¿Los objetivos de la Seguridad de la Información están planificados mediante? -Asignación de responsabilidades -Cronograma de ejecución temporal -Método de evaluación		
3.-	¿Se han integrado los objetivos de la Seguridad de la Información en los procesos de la organización teniendo en cuenta las funciones principales dentro de la Organización?		
7	Soporte		
7.1	**Recursos**		
1.-	¿Se identifican y asignan los recursos necesarios para el SGSI?		
7.2	**Competencia**		
1.-	¿Se evalúa la competencia en materias de Seguridad de la Información para personas que efectúan tareas que puedan afectar a la seguridad?		
2.-	¿Se mantiene información actualizada sobre la competencia del personal?		
7.3	**Concienciación**		
1.-	¿El personal está involucrado y es consciente de su papel en la Seguridad de la Información?		
2.-	¿Existe conciencia de los daños que se pueden producir de no seguir las pautas de la Seguridad de la Información?		
7.4	**Comunicación**		
1.-	¿Se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno?		
2.-	¿Existe un proceso para comunicar las deficiencias o malas prácticas en la seguridad de la Información?		
7.5	**Información Documentada**		
1.-	¿Se dispone de la documentación requerida por la norma más la requerida por la organización incluyendo? -La política de la Seguridad de la Información y el alcance del Sistema de Gestión -Los procesos principales de la seguridad de la Información -Los Documentos exigidos por la Norma ISO 27001 incluyendo registros -Los Documentos propios de Seguridad de la Información identificados por la empresa (instrucciones técnicas etc.)		
2.-	¿Existe un control documental donde se verifica? -Quien publica el documento -Quien lo autoriza y como se revisan -Formatos y Soportes de publicación -Su almacenamiento y protección		
3.-	¿Se controlan los documentos de origen externo?		

8	Operación	SI	NO
8.1	**Control Operacional**		
1.-	¿Los procesos de seguridad de la Información están documentados para controlar que se realizan según lo planificado?		
2.-	¿Existe un proceso para evaluar los riesgos en la Seguridad de la Información antes de realizar cambios en el Sistema de Gestión o procesos de Seguridad?		
3.-	¿Se establecen medidas y planes para mitigar los riesgos en la Seguridad de la Información ante cambios realizados?		
4.-	¿Se identifican y controlan los procesos externalizados en cuanto a los riesgos para la Seguridad de la Información?		
8.2	**Análisis de riesgos de la Seguridad de la Información**		
1.-	¿Se ha establecido un proceso documentado de análisis y evaluación de riesgos para la Seguridad de la Información donde se identifique? -El propietario del riesgo -La importancia del riesgo o nivel de impacto -La probabilidad de ocurrencia		
8.3	**Tratamiento de riesgos de la Seguridad de la Información**		
1.-	¿Se ha implementado un plan de tratamiento de riesgos dónde? -Los propietarios del riesgo están informados y han aprobado el plan -Se documentan los resultados		
2.-	¿Se identifican todos los controles necesarios para mitigar el riesgo justificando su aplicación?		
3.-	¿Se documenta el nivel de aplicación de todos los controles a aplicar?		
9	**Evaluación del desempeño**		
9.1	**Seguimiento y medición**		
1.-	¿Se ha establecido un proceso continuo de monitoreo de los aspectos clave de la seguridad de la información teniendo en cuenta los controles para la seguridad de la información?		
2.-	¿Se ha establecido un proceso documentado para evaluar los resultados de las mediciones y de que estos resultados son tomados en cuenta por los responsables tanto de los procesos como de la Seguridad de la Información?		
9.2	**Auditorías Internas**		
1.-	¿Se ha establecido una programación de Auditorías Internas y asignado responsables?		
2.-	¿Se ha definido el alcance y los requisitos para el informe de auditoría?		
3.-	¿Se consideran acciones correctivas y propuestas de cambio en los informes de auditoría?		
9.3	**Informe de Revisión por la Dirección**		
1.-	¿Existe una programación para los informes de la dirección y existe constancia de su realización periódica?		
2.-	¿Se documentan los resultados de los informes y la dirección se implica tanto en su conocimiento como en la toma de decisiones sobre los aspectos cruciales para el SGSI?		

10	Mejora	SI	NO
10.1	**No Conformidades y acciones correctivas**		
1.-	¿Existe un procedimiento documentado para identificar y registrar las no conformidades y su tratamiento?		
2.-	¿Dentro de las acciones correctivas existe una diferenciación entre acciones correctivas sobre la no conformidad y sobre las causas de la misma?		
10.2	**Mejora continua**		
1.-	¿Existe un proceso para garantizar la mejora continua del SGSI identificando las oportunidades de mejora?		

ANEXO 9. RESULTADOS DE LA ENCUESTA DE CUMPLIMIENTO DE NORMA ISO/IEC 27001:2013

	La Organización y su Contexto								Liderazgo								Planificación							
Individuo	¿Está	¿Se h	¿Se h	¿Se h	¿Exist	¿Exist	¿Se h	¿El 1s	¿Se har	¿La	¿La	¿Se	¿Se	¿Se	¿Se	¿Se	¿El pl	¿Se id	¿Se h	¿Se h	¿Se m	¿Se h	objet	¿Se h
1	1	0	0	1	0	0	0	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	1	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	1	0	0	1	1	1
4	1	1	1	1	0	0	0	0	0	1	1	0	1	1	0	1	1	0	0	0	0	0	0	0	1
5	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	0	1	1	1	1	1
6	1	1	1	0	0	0	0	0	1	1	0	1	1	1	0	1	1	0	0	0	0	0	0	1	1
7	1	1	1	1	1	1	1	0	1	1	0	1	1	1	0	1	1	1	0	1	0	1	1	0	1
8	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1
9	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0
10	0	0	0	1	1	1	1	0	0	1	0	1	0	0	0	1	0	1	1	1	1	1	1	0	1
11	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	9	9	9	9	6	6	6	5	8	11	6	9	7	9	6	10	9	7	7	7	5	5	8	6	9
Población	11								11									11							
Total máximo	88								99									88							
Total	59								75									54							
%	0.67								0.76									0.61							

Soporte										Operación								Evaluación del desempeño							Mejora		
¿Se	¿Se	¿Se	¿El	¿Exi	¿Se	¿Exi	disp	¿Exi	¿Se	¿Los	¿Exist	¿Se e	¿Se ic	estab	¿Se h	¿Se ic	¿Se d	¿Se h	¿Se h	¿Se h	¿Se h	¿Se c	¿Exis	¿Se c	¿Existe ui	¿Dentro	¿Existe ui
1	1	1	1	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0
1	1	1	1	1	1	0	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	0	1	1	0	1
1	0	0	1	1	0	0	1	1	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	1	1	1	1	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	1	0	0	0	0	0
1	1	1	1	1	1	1	0	1	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	1	1	1
1	1	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	0	0	1	0	1	0	1	0	0	0
1	1	0	0	0	0	0	0	1	1	1	1	0	0	0	1	1	1	1	0	0	0	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
10	9	9	9	9	8	6	5	8	6	7	7	7	9	6	7	7	7	6	5	6	5	8	4	6	6	4	5
11										11								11							11		
110										88								77							33		
79										57								40							15		
0.718										0.65								0.52							0.45		

ANEXO 10. ENCUESTA DE CUMPLIMIENTO DE CONTROLES, ANEXO A ISO/IEC 27001:2013

Cláusula	ANEXO A ISO 27001
A5	**Políticas de Seguridad de la Información**
A5.1	**Dirección de gestión para la seguridad de la información**
1.-	¿La dirección ha publicado y aprobado las políticas sobre la Seguridad de la Información acordar con los requisitos del negocio?
2.-	¿Existe un proceso planificado y verificable de revisión de las políticas de Seguridad de la información?
A6	**Organización de la Seguridad de la Información**
A6.1	
1.-	¿Se han asignado y definido las responsabilidades sobre la seguridad de la Información en las distintas tareas o actividades de la organización?
2.-	¿Se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos?
3.-	¿Existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con la Seguridad de la Información?
4.-	¿Existen medios y se han establecido contactos con grupos de interés y asociaciones relacionadas con la seguridad de la información para mantenerse actualizado en noticias e información sobre Seguridad?
5.-	¿Existen requisitos para afrontar cuestiones sobre la seguridad de la información en la gestión de proyectos de la organización?
A6.2	**Dispositivos Móviles y Teletrabajo**
1.-	¿Se consideran requisitos especiales para la Seguridad de la Información en la utilización de dispositivos móviles?
2.-	¿Se aplican los criterios de Seguridad para los accesos de teletrabajo?

A7	**Seguridad en los Recursos Humanos**
A7.1	**Antes de contratar a un empleado**
1.-	¿Se investigan los antecedentes de los candidatos? -Formación -Experiencia -Verificar Titulación -Referencias
1.-	¿Se incluyen cláusulas relativas a la Seguridad de la Información en los contratos de trabajo?
A7.2	**Durante el contrato**
1.-	¿El cumplimiento de las responsabilidades sobre la Seguridad de la Información es exigida de forma activa a empleados y contratistas?
2.-	¿Existen procesos de información, formación y sensibilización sobre las responsabilidades sobre la Seguridad de la Información?
3.-	¿Existe un plan disciplinario donde se comunica a los empleados y contratistas las consecuencias de los incumplimientos sobre las políticas de la Seguridad de la Información?
A7.3	**Terminación del contrato**
1.-	¿Existe un procedimiento para garantizar la Seguridad de la Información en los cambios de empleo, puesto de trabajo o al finalizar un contrato?
2.-	¿Se definen responsabilidades sobre la Seguridad de la información que se extiendan más allá de la finalización de un contrato como por ejemplo cuestiones relativas a la confidencialidad de la Información?
A8	**Gestión de Activos**
A8.1	**Responsabilidad sobre los Activos**
1.-	¿Se ha realizado un inventarios de activos que dan soporte al negocio y de Información?
2.-	¿Se ha identificado al responsable de cada activo en cuanto a su seguridad?
3.-	¿Se han establecido normas para el uso de activos en relación a su seguridad?
4.-	¿Existe un procedimiento para la devolución de activos cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato?
A8.2	**Clasificación de la Información**
1.-	¿Se clasifica la información según su confidencialidad o su importancia en orden a establecer medidas de seguridad especificas?
2.-	¿Los activos de información son fácilmente identificables en cuanto a su grado de confidencialidad o su nivel de clasificación?
3.-	¿Existen procedimientos para el manipulado de la información de acuerdo a su clasificación?
A8.3	**Manipulación de Soportes**
1.-	¿Existen controles establecidos para aplicar a soportes extraíbles? -Uso -Cifrado -Borrado -Etc.
2.-	¿Existen procedimientos establecidos para la eliminación de soportes?
3.-	¿Existen procedimientos para el traslado de soportes de información para proteger su seguridad? -Control de salidas -Cifrado etc.

A9	Control de Acceso
A9.1	**Requisitos generales para el control de acceso**
1.-	¿Existe una política para definir los controles de acceso a la información que tengan en cuenta el acceso selectivo a la información según las necesidades de cada actividad o puesto de trabajo?
2.-	¿Se establecen accesos limitados a los recursos y necesidades de red según perfiles determinados?
A9.2	**Accesos de Usuario**
1.-	¿Existen procesos formales de registros de usuarios?
2.-	¿Existen procesos formales para asignación de perfiles de acceso?
3.-	¿Se define un proceso específico para la asignación y autorización de permisos especiales de administración de accesos?
4.-	¿Se ha establecido una política específica para el manejo de información clasificada cono secreta ? en cuanto a: -Autenticación -Compromisos
5.-	¿Se establecen periodos concretos para renovación de permisos de acceso?
6.-	¿Existen un proceso definido para la revocación de permisos cuando se finalice una actividad, puesto de trabajo o cese de contratos?
A9.3	**Responsabilidades de los usuarios**
1.-	¿Se establecen normas para la creación y salvaguarda de contraseñas de acceso?
A9.4	**Control de acceso a sistemas y aplicaciones**
1.-	¿Se establecen niveles y perfiles específicos de acceso para los sistemas de Información de forma que se restringa la información a la actividad específica a desarrollar?
2.-	¿Se han implementado procesos de acceso seguro para el inicio de sesión considerando limitaciones de intentos de acceso, controlando la información en pantalla etc.?
3.-	¿Se establecen medidas para controlar el establecimiento de contraseñas seguras?
4.-	¿Se controla la capacitación y perfil de las personas que tienen permisos de administración con perfiles bajos de Seguridad?
5.-	¿Se restringe el acceso a códigos fuente de programas y se controla cualquier tipo de cambio a realizar?

A10	Criptografía
A10.1	**Control criptográfico**
1.-	¿Existe una política para el establecimiento u yo de controles criptográficos?
2.-	¿Existe un control del ciclo de vida de las claves criptográficas?
A11	**Seguridad Física y del entorno**
A11.1	**Áreas de Seguridad**
1.-	¿Se establecen perímetros de seguridad física donde sea necesario con barreras de acceso?
2.-	¿Existen controles de acceso a personas autorizadas en áreas restringidas?
3.-	¿Se establecen medidas de seguridad para zonas de oficinas para proteger la información de pantallas etc. en áreas de accesibles a personal externo?
4.-	¿Se controla o supervisa la actividad de personal que accede a áreas seguras?
5.-	¿Se controlan las áreas de Carga y descarga con procedimientos de control de mercancías entregadas etc.?
A11.2	**Seguridad de los equipos**
1.-	¿Se protegen los equipos tanto del medioambiente como de accesos no autorizados?
2.-	¿Se protegen los equipos contra fallos de suministro de energía?
3.-	¿Existen protecciones para los cableados de energía y de datos?
4.-	¿Se planifican y realizan tareas de mantenimiento sobre los equipos?
5.-	¿Se controlan y autorizan la salida de equipos, aplicaciones etc. Que puedan contener información?
6.-	¿Se consideran medidas de protección específicas para equipos que se utilicen fuera de las instalaciones de la propia empresa?
7.-	¿Se establecen protocolos para proteger o eliminar información de equipos que causan baja o van a ser reutilizados?
8.-	¿Se establecen normas para proteger la información de equipos cuando los usuarios abandonan el puesto de trabajo?
9.-	¿Se establecen reglas de comportamiento para abandonos momentáneos o temporales del puesto de trabajo?

A12	Seguridad en las Operaciones
A12.1	**Procedimientos y responsabilidades**
1.-	¿Se documentan los procedimientos y se establecen responsabilidades?
2.-	¿Se controla que la información sobre procedimientos se mantenga actualizada?
3.-	¿Se dispone de un procedimiento para evaluar el impacto en la seguridad de la información ante cambios en los procedimientos?
4.-	¿Se controla el uso de los recursos en cuanto al rendimiento y capacidad de los sistemas?
5.-	¿Los entornos de desarrollo y pruebas están convenientemente separados de los entornos de producción?
A12.2	**Protección contra software malicioso**
1	¿Existen sistemas de detección para Software malicioso o malware?
A12.3	**Copias de Seguridad**
1.-	¿Se ha establecido un sistema de copias de seguridad acordes con las necesidades de la información y de los sistemas?
A12.4	**Registros y supervisión**
1.-	¿Se realiza un registro de eventos? -Intentos de acceso fallidos/exitosos -Desconexiones del sistema -Alertas de fallos Etc.
2.-	¿Se ha establecido un sistema de protección para los registros mediante segregación de tareas o copias de seguridad?
3.-	¿Se protege convenientemente y de forma específica los accesos o los de los administradores?
4.-	¿Existe un control de sincronización de los distintos sistemas?
A12.5	**Control del Software**
1.-	¿Las instalaciones de nuevas aplicaciones SW o modificaciones son verificadas en entornos de prueba y existen protocolos de seguridad para su instalación?
A12.6	**Vulnerabilidad Técnica**
1.-	¿Se establecen métodos de control para vulnerabilidades técnicas "hacking ético" etc.?
2.-	¿Se establecen medidas restrictivas para la instalación de Software en cuanto a personal autorizado evitando las instalaciones por parte de usuarios finales?
A12.6	**Auditorias de Sistemas de Información**
1.-	¿Existen mecanismos de auditorías de medidas de seguridad de los sistemas?
2.-	¿Se establecen protocolos específicos para desarrollo de auditorías Software considerando su impacto en los sistemas?
A13	**Seguridad en las Comunicaciones**
A13.1	**Seguridad de Redes**
1.-	¿En el entorno de red se gestiona la protección de los sistemas mediante controles de red y de elementos conectados?
2.-	¿Se establecen condiciones de seguridad en los servicios de red tanto propios como subcontratados?
3.-	¿Existe separación o segregación de redes tomando en cuenta condiciones de seguridad y clasificación de activos?
A13.2	**Intercambio de Información**
1.-	¿Se establecen políticas y procedimientos para proteger la información en los intercambios?
2.-	¿Se delimitan y establecen acuerdos de responsabilidad en intercambios de información con otras entidades?
3.-	¿Se establecen normas o criterios de seguridad en mensajería electrónica?
4.-	¿Se establecen acuerdos de confidencialidad antes de realizar intercambios de información con otras entidades

A14	**Adquisición, desarrollo y mantenimiento de sistemas de información**
A14.1	**Intercambio de Información**
1.-	¿Se definen y documentan los requisitos de Seguridad de la Información para los nuevos sistemas de Información?
2.-	¿Se especifican los requisitos de Seguridad de la información en el diseño de nuevos sistemas?
3.-	¿Se consideran requisitos de seguridad específicos para accesos externos o de redes públicas a los sistemas de información?
4.-	¿Se establecen medidas de protección para transacciones Online?
A14.2	**Seguridad en los procesos de Soporte**
1.-	¿Se establecen procedimientos que garanticen el desarrollo seguro del Software?
2.-	¿Se gestiona el control de cambios en relación al impacto que puedan tener en los sistemas?
3.-	¿Se establecen procedimientos de revisión después de efectuar cambios o actualizaciones?
4.-	¿Se establecen procesos formales para cambios en versiones o nuevas funcionalidades para Software de terceros?
5.-	¿Se definen políticas de Seguridad de la Información en procesos de ingeniería de Sistemas?
6.-	¿Se realiza una evaluación de riesgos para herramientas de desarrollo de Software?
7.-	¿Se acuerdan los requisitos de seguridad de la Información para Software desarrollado por terceros?
8.-	¿Se realizan pruebas funcionales de seguridad de los sistemas antes de su fase de producción?
9.-	¿Se establecen protocolos y pruebas de aceptación de sistemas para nuevos sistemas y actualizaciones?
A14.3	**Datos de prueba**
1.-	¿Se utilizan datos de prueba en los ensayos o pruebas de los sistemas?
A15	**Relación con Proveedores**
A15.1	**Seguridad en la Relación con Proveedores**
1.-	¿Existe una política de Seguridad de la información para proveedores que acceden a activos de la información de la empresa?
2.-	¿Se han establecido requisitos de seguridad de la información en contratos con terceros¿
3.-	¿Se fijan requisitos para extender la seguridad de la información a toda la cadena de suministro?
A15.1	**Gestión de servicios externos**
1.-	¿Se controla el cumplimiento de los requisitos establecidos con proveedores externos?
2.-	¿Se controlan los posibles impactos en la seguridad ante cambios de servicios de proveedores externos?
A16	**Gestión de incidentes de seguridad de la información**
A16.1	**Gestión de incidentes de seguridad de la información y mejoras.**
1.-	¿Se definen responsabilidades y procedimientos para responder a los incidentes de la Seguridad de la Información?
2.-	¿Se han implementado canales adecuados para la comunicación de incidentes en la seguridad de la Información?
3.-	¿Se promueve y se hayan establecidos canales para comunicar o identificar puntos débiles en la Seguridad de la Información?
4.-	¿Se ha establecido un proceso para gestionar los incidentes en la Seguridad de la Información?
5.-	¿Existen mecanismos para dar respuesta a los eventos de la Seguridad de la Información?
6.-	¿La información que proporcionada por los eventos en la Seguridad de la información son tratados para tomar medidas preventivas?
7.-	¿Existe un proceso para recopilar evidencias sobre los incidentes en la seguridad de la Información?

A17	Gestión de la Continuidad del Negocio
A17.1	**Continuidad de la seguridad de la información.**
1.-	¿Se ha elaborado un plan de continuidad del negocio ante incidentes de Seguridad de la Información?
2.-	¿Se ha implementado las medidas de recuperación previstas en el plan de Continuidad del Negocio?
3.-	¿Se han verificado o probado las acciones previstas en el plan de Continuidad del Negocio?
A17.2	**Redundancias**
1.-	¿Se ha evaluado la necesidad de redundar los activos críticos de la Información?
A18	**Cumplimiento**
A18.1	**Cumplimiento de los requisitos legales y contractuales.**
1.-	¿Se han identificado las legislaciones aplicables sobre protección de datos personales y su cumplimiento? -LOPD -Leyes para comercio Electrónico -Transacciones Bancarias -Información Protegida -Otras propias del negocio o actividad -Ley general de Telecomunicaciones
2.-	¿Existen procedimientos implementados sobre la propiedad intelectual?
3.-	¿Se establecen criterios para clasificación de registros y medidas de protección según niveles?
4.-	¿Se establecen medidas para la protección de datos personales de acuerdo con la legislación vigente?
5.-	¿Si se utiliza el cifrado, se establecen controles criptográficos de acuerdo a la legislación?
A18.2	**Revisiones de la Seguridad de la Información**
1.-	¿Se revisan los controles de la Seguridad de la Información por personal independiente a los responsables de implementar los controles?
2.-	¿Se revisa periódicamente el cumplimiento de las políticas y controles de la Seguridad de la información?
3.-	¿Se realizan evaluaciones sobre el correcto funcionamiento de las medidas técnicas de protección para la seguridad de la información?

ANEXO 11. RESULTADO DE CUMPLIMIENTO DE CONTROLES, ANEXO A ISO/IEC 27001:2013

A6 \| A14 \| A16

Correo electrónico	Nombre	¿Se	¿Se ha	¿Ex	¿Ex	¿Ex	¿Se	¿Se
allan.vasquez@elcatex.com	Allan Vásquez	3	3	3	3	3	2	3

Correo electrónico	Nombre	¿Se	¿Se (	¿Se	¿Se	¿Se	¿Se	¿Se	¿Se	¿Se	¿Se	¿Se	¿Se	¿Se
allan.vasquez@elcatex.com	Allan Vásquez	4	4	3	3	4	3	3	4	2	3	2	2	4

Correo electrónico	Nombre	¿Se	¿Se han	¿Se	¿Se	¿Exi	¿La	¿Exi
allan.vasquez@elcatex.com	Allan Vásquez	3	3	3	3	4	4	3

GRADO DE CUMPLIMIENTO	NIVELES
Totalmente de acuerdo	5
De acuerdo	4
Neutral	3
En desacuerdo	2
Totalmente en desacuerdo	1

TOTAL		TOTAL		TOTAL	
0	0%	0	0%	0	0%
0	0%	5	38%	2	29%
6	86%	5	38%	5	71%
1	14%	3	23%	0	0%
0	0%	0	0%	0	0%
7	100%	13	100%	7	100%

	A8										A10		A12																A13						
Individuo	s q	de c	usc	a f	import		on	rt	cio	ac	im	de vi	tos	e pr	la	nto	nie	pa	rde	ido	gist	esp	niz	das	vu	nto	de	a	ter	s servi	n c	pa	da	de	re
Enrique O	5	5	5	3	5	4	5	4	3	3	5	5	4	5	4	4	4	5	5	3	3	5	4	5	5	5	4	4	5	5	4	5	4	5	3
C Mejia	4	4	5	4	4	3	4	5	4	4	3	3	4	4	4	5	5	5	5	5	5	4	4	4	5	4	4	4	4	4	4	4	5	5	4

GRADO DE CUMPLIMIENTO	NIVELES
Totalmente de acuerdo	5
De acuerdo	4
Neutral	3
En desacuerdo	2
Totalmente en desacuerdo	1

TOTAL	%
7	35%
9	45%
4	20%
0	0%
0	0%
20	100%

TOTAL	
2	50%
0	0%
2	50%
0	0%
0	0%
4	100%

TOTAL	
14	44%
16	50%
2	6%
0	0%
0	0%
32	100%

TOTAL	%
6	43%
7	50%
1	7%
0	0%
0	0%
14	100%

GLOSARIO

Ataque: Intentar destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer un uso no autorizado de un activo.

Autenticidad: Propiedad que una entidad es lo que dice ser.

Confidencialidad: Propiedad por la que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados.

Conformidad: Cumplimiento de un requisito.

Control de acceso: Medios para garantizar que el acceso a los activos esté autorizado y restringido según los requisitos comerciales y de seguridad.

Consecuencia: Resultado de un evento que afecta a los objetivos.

Disponibilidad: Propiedad de ser accesible y utilizable a solicitud de una entidad autorizada.

Efectividad: En qué medida se realizan las actividades planificadas y se logran los resultados planificados.

Incidente de seguridad de la información: Un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información

Mejora Continua: Actividad recurrente para mejorar el rendimiento.

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información.