UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
Modelo de evaluación del nivel de madurez de la seguridad de la información
Línea de Investigación:
SEGURIDAD INFORMÁTICA
Campo amplio de conocimiento:
TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
Autor/a:
Luis Antonio Vallejo Rodríguez
Tutor/a:
Mg. Pablo Marcel Recalde Varela

Quito - Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, Pablo Marcel Recalde Varela con C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado: **Modelo de evaluación del nivel de madurez de la seguridad de la información**.

Elaborado por: Luis Antonio Vallejo Rodríguez, de C.I: 171244408-0, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2023

Firmado electrónicamente por:
PABLO MARCEL
RECALDE VAREIA

Firma

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

Este trabajo de investigación está enfocado en el desarrollo de una estructura que permita evaluar la madurez en gestión a los procesos de seguridad de la información para cualquier organización del sector asegurador en el Ecuador, para esto, el análisis estará fundamentado en la identificación de amenazas, vulnerabilidades y fortalezas que tienen las empresa de este tipo a la hora de enfrentar incidentes de seguridad y su capacidad de resiliencia, por otro lado, esta estructura permitirá conocer las capacidades de gobernanza, el nivel de cultura organizacional con los usuarios y socios estratégicos en la concienciación de buenas prácticas de seguridad.

De esta forma se pretende fortalecer los controles existentes y aplicar estrategias basadas en las principales normativas vigentes y de impacto mundial en la gestión de la seguridad de la Información e informática como:

- **ISO 27000**

Nace de la Oíganización Inteínacional de Noímalización (ISO), paía la familia de las 27000 se descíiben los difeíentes elementos a consideíaí en la gestión a los difeíentes píocesos de seguíidad de la infoímación en una oíganización de cualquieí tipo y capacidad, estas podíían seí, píivadas o públicas, con o sin fines de lucío.

Esta noíma al seí paíte de la familia ISO ha venido siendo elaboíada y actualizada poí los mejoíes exponentes, oíganizaciones públicas o píivadas en el ámbito de la seguíidad de la infoímación y píopoíciona una guía metodológica paía implementaí mecanismos de gestión y valoíación de íiesgos en la seguíidad de la infoímación. (Advisera, 2021)

- **SysAdmin Audit Network Security (SANS)**

Evalúa las normas de seguridad informática vigentes para cualquier tipo de organización y propone mejoras a todos los tipos de control existente mediante una guía general de implementación por tipo de industria. (PCI, 2008)

- **NIST 800**

Es parte de una familia de publicaciones del Instituto Nacional de Estándares y Tecnología en EEUU, NIST por sus siglas en Inglés, que refinan y elabora métricas y/o estándares para el óptimo desempeño en el avance y desarrollo tecnológico; en este caso NIST 800 se encarga de garantizar una adecuada gestión de seguridad a la tecnología y sus actores, estos estándares son utilizados por las diferentes agencias federales y han sido

tomadas como referencia para implementar mecanismos de regulación en la Ley Federal en la Administración de la Seguridad de la Información (FISMA), también toma como referencia otros tipos de programas que están diseñados para proteger y garantizar el uso de los activos tecnológicos en todo su ciclo de vida; por otro lado promueve a la seguridad de la información como parte de los deberes de un estado (Technopedia, 2021)

- **PCI 3.0**

Es un estándar desarrollado para fomentar y mejorar la seguridad de los datos en todo su ciclo de vida y facilitar la adopción de medidas de seguridad a nivel de vanguardia y vigentes del mercado. Asimismo, proporcionan una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los clientes. (PCI, 2013)

Según la investigación realizada por Figueroa et al. (2018), propone la necesidad de realizar un análisis documental de la seguridad de información por tipo de industria con la finalidad de mostrar las brechas de controles y objetivos que tiene cada segmento empresarial, por esto, este trabajo investigativo se enfoca en el segmento de las empresas del segmento asegurador del Ecuador por ser un tipo de industria que realiza tratamiento de información en todo nivel, y por tanto debe contar con cumplimiento regulatorio en materia de seguridad y auditorías de ley, convirtiéndose en un sector que debe ser atendido mediante métricas más efectivas y aterrizadas a la realidad.

Los principales problemas que presentan las empresas de seguros en temas relacionados con la seguridad de la información, es la falta de controles y gestión de accesos en la seguridad perimetral, siendo esta una de las principales brechas que desembocan en incidentes de seguridad que afecten a cualquier activo de información, de la misma forma, muchas de las instituciones no cuentan con antivirus o herramientas avanzadas de análisis que prevean ataques más sofisticados.

La comunicación y concienciación del personal en temas relacionados a la seguridad de la información, deberes y responsabilidades en el uso de las tecnologías de la información, se convierte en una de las principales estrategias a la hora de aplicar buenas prácticas.

Problema de investigación

Con el continuo avance tecnológico en todos los ámbitos de la industria es de gran importancia para las empresas contar con métodos que permita evaluar o valorar la madurez de seguridad de la información e informática basándose en las mejores prácticas y estándares internacionales y que además, permita identificar si el proceso vigente es efectivo y si está ajustado a una constante mejora, dado que, una práctica muy habitual en las

entidades es basar su confianza de seguridad de datos en la percepción y en el uso de herramientas tecnológicas aisladas a una estrategia y planificación basada en riesgos.

Esto viene a generar pérdidas sustanciales en las organizaciones debido a incidentes de seguridad que afectan no solo a los principios de seguridad sobre los activos de información (confidencialidad, integridad y disponibilidad), también generan impactos reputacionales y económicos. Para mediados del año 2022 solo en América Latina se registraron 746.000 ataques informáticos, un 60% más de los registrados entre 2019 y 2021, poniendo en evidencia el déficit de gestión y gobernanza de la seguridad informática en la industria. (El Nuevo día, 2022)

En la actualidad muchas empresas y, en especial, las empresas del sector asegurador del Ecuador no cuentan con un método que permita evaluar la madurez de los procesos y procedimientos de seguridad de la información o el estado de sus controles ante amenazas vigentes y en constante desarrollo, esto provoca evidentes brechas de seguridad que generan pérdidas, accesos no autorizados o indisponibilidad de servicios, puesto que, estar listos ante estas amenazas es clave para toda organización, conocer el estado de los controles y mecanismos de protección viene a ser el punto de partida para cualquier estrategia de seguridad o gestión de riesgos.

Con base a esto, surge la siguiente interrogante de la problemática:

- ¿Cómo evaluar el nivel de madurez de seguridad informática del sector asegurador del Ecuador?

Objetivos

Objetivo general

Elaborar un modelo de evaluación del nivel de madurez de seguridad de la información para el sector asegurador del Ecuador mediante una estructura que toma de referencia las mejores prácticas de seguridad, ciberseguridad y estrategias o estándares internacionales como NIST, SANS, ISO, PCI.

Objetivos específicos

- Fundamentar bibliográficamente el nivel de madurez adecuado de la seguridad de la información en una compañía.
- Determinar los inconvenientes que tienen las empresas más grandes del sector asegurador al momento de evaluar sus controles y mecanismos de seguridad.
- Desarrollar un modelo para valorar la madurez de la seguridad de la información.
- Validar el impacto de los resultados de madurez de seguridad de la información propuestos en el modelo.

Vinculación con la sociedad y beneficiarios directos

Dentro de los objetivos que se proponen para el desarrollo sostenible, mismo que es dispuesto por Las Naciones Unidas (UN), este proyecto se enmarca en cubrir el Objetivo 9: Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación.

Actualmente las empresas para la toma de decisiones se basan en la información generada de sus operaciones, herramientas tecnológicas y/o mecanismos de procesamiento existentes, y en la actualidad también en la fundamentación de los datos alojados en centros de datos externos o nubes de Internet, donde se almacena todo tipo de información confidencial o personal de clientes, proveedores, servicios o demás socios estratégicos, por esta razón esta información y sus mecanismos de tratamiento deben estar debidamente protegidos contra alteraciones, pérdidas o accesos no autorizados; brindando de características de resiliencia en los servicios prestados ,por ello, surge la necesidad de implementar un modelo que permita valorar el nivel de madurez de los controles de seguridad implementados y que garanticen principios de privacidad y protección.

Para evaluar los controles, procesos, herramientas y garantizar una adecuada gestión de seguridad de la información, se realizará una estructura que permitirá evaluar el nivel de madurez en función de un compendio de 24 controles de seguridad, los cuales, que

se basan en estándares internacionales para la seguridad y ciberseguridad, tales como, SANS, NIST CF, PCI 3.0 e ISO 27000, permitiendo beneficios en la priorización y enfoque de acciones correctivas o de implementación con altos resultados, este modelo toma como base los principios descritos en ISO 27001 y 27032, de esta forma se agrupan estándares de estas normas con los propuestos en las normas antes mencionadas.

Asimismo, este modelo describe mediante una métrica la madurez en los controles de seguridad de la información e informática, estructurada por niveles, los cuales, ayudarán a gestionar de mejor manera los controles a los procesos críticos, a dar tratamiento los controles previstos desde la evaluación de riesgos. Este análisis permitirá a las compañías identificar los puntos de mejora conforme a las debilidades presentadas y las posibles brechas en las cuales el tratamiento requiere más esfuerzo.

Finalmente, el modelo permitirá tener una visión más estratégica de las actividades de seguridad a realizar e identificará las vulnerabilidades de sus controles vigentes, también, generar una visualización de sus fortalezas y debilidades permitirá a las compañías a estar mejor preparadas ante posibles ataques cibernéticos o actividades dirigidas por *Insiders.* Todo esto acorde a los objetivos de desarrollo sostenible como es el de Industria, Innovación e Infraestructura (ODS 9)

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

Contextualización general del estado del arte

Haciendo referencia al artículo científico desarrollado por Holguín y Lema (2019), mencionan que el avance de la tecnología debe ir ligado a la gestión en la seguridad, pues sin ella esta podría verse comprometida, y adicional sugieren gestionar los riesgos de ataques cibernéticos por parte de usuarios de la red malintencionados o insiders, por lo cual, es de vital importancia realizar una análisis de riesgos preventivo para identificar las posibles amenazas, ataque o vulnerabilidades, como propuesta indican un Modelo para Medir la Madurez del Análisis de Riesgos de los Activos de Información en este contexto empresarial. Asimismo, utilizaron MAGERIT, OCTAVE y MEHARI como metodología para el análisis de riesgos y aplicaron entrevistas a siete empresas navieras con el objetivo de identificar su nivel de madurez de la información, en la cual, se determinó que estas empresas requieren un modelo para medir la madurez del análisis de información y prevenir pérdidas de la información a futuro.

Según el artículo de investigación desarrollado en la Universidad Tecnológica Empresarial de Guayaquil por López (2017) donde se planteó diseñar un Modelo de gestión y mejora a los servicios tecnológico de información utilizando como metodología a COBIT v5, misma que está elaborada por la "Asociación de Control y Auditoría de Sistema de Información", asimismo, utilizó la ITIL v3 2011, la cual, facilita la ejecución de los servicios que permitan mejorar los procesos que se realizan dentro de las empresas y de esta forma obtener beneficios como alta confiabilidad, continuidad, disponibilidad, capacidad de respuesta, mejora del tiempo de respuesta ante posibles amenazas y contar con un grupo más preparado para reducir las amenazas que se presentan en las organizaciones.

Tomando como referencia el artículo previo a la obtención de Magíster en Auditoría de Tecnologías de la Información en la ciudad de Samborondón, presentado por Capelo y Sotomayor (2018), plantearon desarrollar y aplicar un modelo que evalúe la madurez en la Gestión de Seguridad de la Información para las Instituciones de Salud Pública de la ciudad de Cuenca, la cual, utiliza las tecnologías de la información para optimizar los servicios prestados, generar reducción de costos y tomar de decisiones inmediatas y oportunas, sin embargo, tiene una debilidad que no cuenta con los estándares y políticas que aseguren la confiabilidad, disponibilidad e integridad de la seguridad de la información que se encuentra en la institución, por esto, se planteó la implementación del modelo para evaluar la madurez de la seguridad de la información en instituciones de salud pública y controlar de forma

periódica los estándares y políticas que salvaguarden la información por medio de la metodología propuesta por Becker et al. (2009).

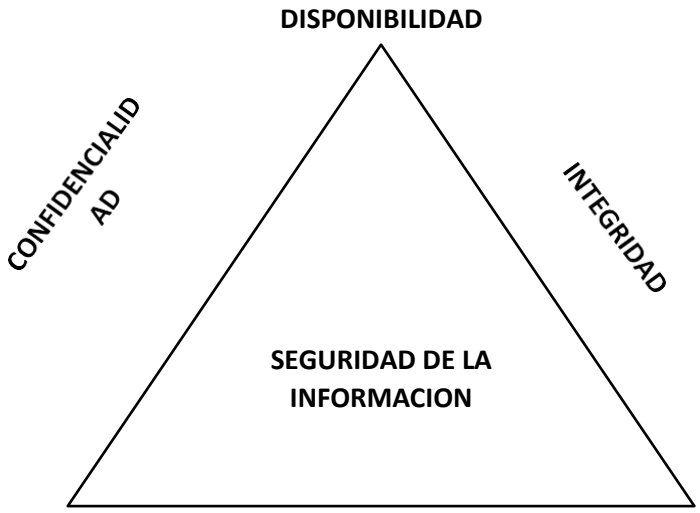
Según la investigación realizada por Ramírez (2021) previo a la obtención de maestría en tecnologías de información y comunicación en la ciudad de Medellín, en el cual, pretendía desarrollar un estrategia que vaya mejorando progresivamente como parte del SGSI en la Alcaldía de Barbosa Antioquia, partió del análisis de las vulnerabilidades que se presentaban en la institución, las cuales, fueron alineadas a las recomendaciones del estado por medio del Ministerio de Tecnología (MINTIC), se planteó estándares y buenas prácticas de la industria tales como ISO 27000 y la NIST para un correcto manejo de la información, utilizada para la prevención de ataques y pérdidas de datos, también, se identifican todas las posibles vulnerabilidades que tiene la arquitectura de la red basada en controles propuestos por NIST SP 800-115, con estas actividades se corrigieron en su mayoría las vulnerabilidades y se implementaron mejoras en los procesos vigentes.

Seguridad de la información

Como se menciona en las normas ISO/IEC 17799 Política de Seguridad (ISOTools Excellence, 2015), Las conductas y buenas Prácticas en la Gestión de la Seguridad de la Información, se establecen mediante un conjunto de políticas, normas, instructivos y/o procedimientos en las que intervienen personas, procesos y sistemas, aplicando un constante monitoreo para asegurar la integridad, confidencialidad y disponibilidad de la información y sus medios de procesamiento.

Figura 1

Triángulo de la seguridad de la información



Nota. Tomado de Infosegur (2022)

Modelo CIA

El modelo segmenta los principios de seguridad de datos en una tríada de protección; Confidencialidad, Integridad y Disponibilidad y fue establecido en el año de 1941, este grupo colegiado en la actualidad cuenta con más de 128.00 miembros (Mifsud, 2012).

La persona que realiza el análisis de la seguridad de la información aprueba cuatro exámenes diseñados para obtener la certificación CIA, uno de los cuatro exámenes hace énfasis en los sistemas de la información donde son evaluadas las experiencias y capacidades en temas como:

- Planeación de auditoría de TI y análisis de evaluaciones anteriores
- Manejo de información y controles asignados a un responsable.
- Evaluaciones en centros de cómputo internos o cluod.
- Auditorías a sistemas operativos y monitoreo a la administración de red.
- Evaluación de todos los sistemas de información críticos de la compañía.
- Auditoría a los nuevos desarrollos de sistemas.
- Auditorías a los controles de telecomunicaciones y redes.

Como se menciona en el artículo desarrollado por Holguín y Lema (2019), con el presente diseño, se logrará medir el identificar las capacidades de los profesionales acerca de los conceptos fundamentales de la seguridad de la información e informática y pondrá en evidencia las mejoras a aplicarse y métodos de protección adecuados que cubran los conceptos de: Confidencialidad, Integridad y Disponibilidad.

- **Confidencialidad**

Es la propiedad que mantiene la información más importante y relevante en secreto, protegiendo que no sea revelada a usuarios no autorizados. La confidencialidad es aplicada a los datos almacenados durante el procesamiento, cuando son transmitidos y en el tránsito de los datos. Identificando así que la confidencialidad es una de las propiedades más importantes de la seguridad de la información (Niño, 2018, pp 14-16).

- **Integridad**

Es la propiedad encargada de garantizar que los datos almacenados o en tránsito no hayan sido manipulados y alterados por usuarios que no son autorizados para hacerlo, con esto se evita la pérdida total o parcial de la información almacenada, procesada o transmitida. La alteración de la información se puede dar cuando un usuario o programa no autorizado modifica o borra los datos relevantes, por lo cual, la integridad es la encargada de garantizar la completitud y exactitud de la información (Niño, 2018).

- **Disponibilidad**

Es una de las propiedades que garantiza que la información siempre se encuentre al alcance de los procesos, personas o aplicaciones que deben acceder a ella. Estos datos sólo estarán disponibles a personas autorizadas en el momento que lo requieran, por un proceso o sistema informático, los controles de seguridad que se utilizan para proteger la información y los canales de la comunicación que son utilizados para su acceso deben estar funcionando correctamente, caso contrario sus controles deben ser revisados (Niño, 2018, pp 16-17).

Gestión de la Seguridad

Acorde a Capelo, M., & Sotomayor, M. (2018), la gestión de la seguridad involucra tres ámbitos importantes:

- **Organización**

Un sistema de información para cualquier compañía viene a formar parte fundamental en su infraestructura, aportando en optimizar las formas de trabajo y las relaciones interpersonales con otros socios estratégicos, convirtiéndose en un activo muy importante dentro de la empresa, por lo que se debe de implementar un plan de seguridad de la información aplicando un plan estratégico de seguridad de la información.

- **Entorno físico**

Es necesario conocer el entorno donde se encuentra ubicada y se da la operatividad de la organización, de este modo se podrá prevenir los riesgos de seguridad que se hayan identificado. También se deben aplicar controles de acceso físico así como lógicos, detección de intrusos, sistemas de bioseguridad, detectores de incendios, sistemas de vigilancia, entre otros. Por otra parte, se deberá revisar que los almacenes de información alojados en sitios propios o de externos cuenten con las respectivas copias de seguridad y que las mismas sean almacenadas con todos los controles antes descritos y de ser posible en sitios alternos que garanticen la disponibilidad.

- **Entorno lógico**

Para un tratamiento adecuado en la gestión de seguridad de la información en cualquier compañía se debe tomar en cuenta la elaboración de políticas y normas de seguridad que abarquen estrategias para cubrir todo tipo de eventos emergentes o catastróficos, mismos que pueden poner en riesgos los servicios, sistemas de información, telecomunicaciones y, en general, la operativa de la compañía.

Por esto, en el entorno lógico se debe identificar y evaluar todos los riesgos, tomando en cuenta los diferentes escenarios en los cuales el entornó lógico puede verse afectado por alguna vulnerabilidad asociada a su ubicación, uso y exposición a condiciones naturales complejas.

Procesos para la gestión del riesgo de la seguridad de la información

El proceso de gestión del riesgo de seguridad de la información identifica las posibles amenazas y vulnerabilidades con las cuales se estimará y valorará la posibilidad de problemas dentro de los diferentes procesos, personas o sistemas de una organización, este

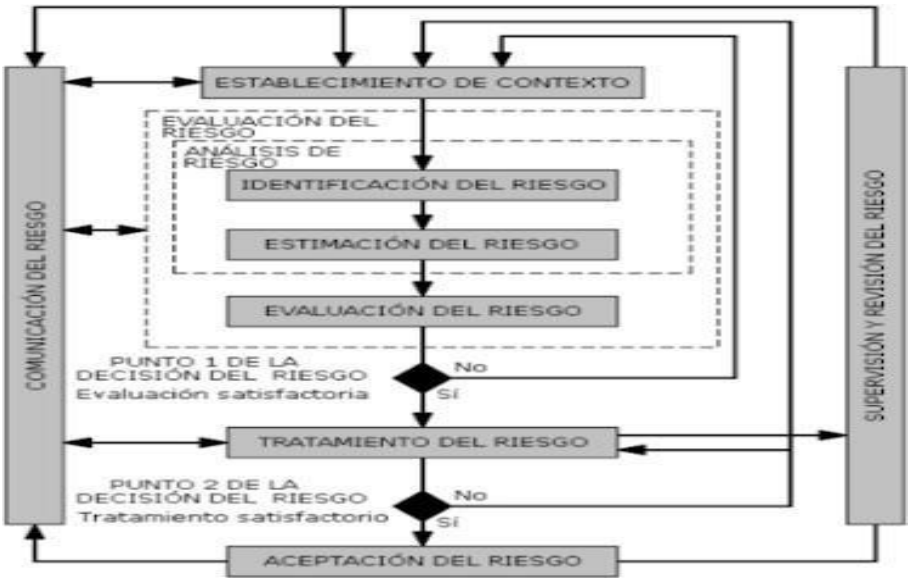
enfoque realiza una valoración que puede incrementar el nivel de riesgo y el detallar las diferentes consecuencias que se generan por el pasar del tiempo.

Este enfoque iterativo genera un balance entre la reducción del tiempo invertido y el esfuerzo requerido para identificar los controles necesarios. Asimismo, cuenta con acciones para la gestión del riesgo de la seguridad de la información. García, J., Huamani, S., & Lomparte, R. (2018):

- Establecimiento del contexto
- Valoración del riesgo
- Tratamiento del riesgo
- Aceptación del riesgo
- Comunicación del riesgo
- Monitoreo y revisión del riesgo

Figura 2

Proceso de gestión del riesgo en la seguridad de la información



Nota. Tomado de ISO27005: 2008

Importancia de la seguridad de la información

En la actualidad existen riesgos y amenazas en internet que son detectadas continuamente y las empresas pueden sufrir pérdidas de la información importante de sus clientes por no tener una correcta seguridad, es por ello, que es necesario abordar este tema, el mismo que puede generar robo de información, pérdidas económicas o de credibilidad con los usuarios, vulnerabilidad ante la competencia, seguridad personal, competencia empresarial, los que podría provocar que la entidad pierda su capital y liquidez final empresarial.

Normativas para medir la seguridad de la información

Según la investigación realizada por Cano y Almanza (2020), se menciona que en los últimos 18 años las herramientas de seguridad que se utilizaron con mayor frecuencia para mantener la seguridad de la información en las empresas son los Firewalls, los cuales, han permitido identificar las fallas de seguridad por medio los protocolos que advierten de nuevas vulnerabilidades institucionales.

Para el desarrollo del presente modelo que busca medir el nivel de madurez de la seguridad de la información se aplicarán las normativas internacionales como con la SANS 6.1, NIST CF, PCI 3.0 y la ISO 27001, las cuales, ayudarán a identificar las fortalezas y vulnerabilidades que tienen los datos dentro de las empresas del sector de aseguradoras más grandes del Ecuador.

Proceso investigativo metodológico

Enfoque de la investigación

Para el desarrollo del presente artículo se realizará un enfoque cualitativo, el mismo que ayudará en la recolección de los datos que permitan identificar las falencias y vulnerabilidades de la información que actualmente se encuentran en el sector de las aseguradoras del Ecuador.

Investigación de campo

Mediante el proceso cualitativo se recolectó la información por medio de entrevistas aplicadas a los propietarios de las empresas para realizar el análisis de los datos e identificar las soluciones del problema.

Investigación Bibliográfica

La investigación bibliográfica permite recolectar información de libros, artículos o tesis referentes al tema de investigación de las bibliotecas tanto físicas como virtuales. (Bernal Torres, 2016)

Para el desarrollo de marco teórico se aplicó la investigación bibliográfica: Sitios Fabricantes, Bibliografía, Blogs, la cual, permitió la recolección de la información de los diferentes repositorios digitales, artículos y libros que fueron de suma importancia para la contextualización general del estado del arte.

Población

La presente investigación se aplicó utilizando como referencia a las 5 empresas más grandes categorizadas por su nivel de Prima Neta Retenida, o capacidad de solvencia en función del número de clientes. Esta información se encuentra pública en la Superintendencia de compañías, estas instituciones permitirán que la recolección de los datos sea más efectiva a fin de identificar las principales vulnerabilidades de seguridad de la información existentes en todo su modelo de negocio.

SUPERINTENDENCIA DE COMPAÑÍAS, VALORES Y SEGUROS

RANKING DE COMPAÑÍAS DE

Este reporte presenta la posición financiera de las compañías de seguros dentro del sistema de seguros privados, en base a la participación

TIPO INSTITUCION: ASEGURADORAS | RAMO: CONSOLIDADOS(VIDA | AÑO: 2023 | MES: ENERO | CUENTA: PRI

	ENERO-2022		
ENTIDAD	PRIMAS NETAS RETENIDAS	%	POSICIÓN
PICHINCHA	15.064.757,84	15,00%	1
CHUBB SEGUROS ECUADOR S.A.	15.029.598,79	15,00%	2
EQUINOCCIAL	13.577.129,57	13,00%	3
AIG METROPOLITANA	7.701.240,41	7,00%	4
ZURICH SEGUROS ECUADOR S.A.	6.521.207,38	6,00%	5
ASEGURADORA DEL SUR	5.861.178,72	6,00%	6
SWEADEN COMPAÑIA DE SEGUROS S.A.	4.190.512,12	4,00%	7

Plan de recolección de la información

Entrevista

La entrevista es realizada a una persona en específico con preguntas abiertas referentes al tema de la investigación, el entrevistado puede responder las interrogantes con toda libertad, mostrando así sus opiniones personales referentes al tema. (Hernández-Sampieri & Mendoza Torres, 2018)

Para la recolección de la información se aplicará una entrevista a los directores de riesgos o posiciones similares que puedan describir las acciones de seguridad dentro de las cinco empresas de seguros más grandes del país, valoradas por la superintendencia de Bancos.

Análisis de resultados

Análisis de la entrevista aplicada a los jefes de las empresas aseguradoras del Ecuador.

Pregunta 1: Tamaño de la empresa.

Según la entrevista aplicada a los gerentes de las cinco aseguradoras más grandes del Ecuador, se identificó que en el tamaño de las empresas se encuentran entre los 300 hasta los 700 usuarios, en esta población está incluida los socios estratégicos, siendo un campo muy amplio para aplicar el estudio, puesto que es un ámbito laboral extenso que debe contar con un modelo o estructura que permita medir el nivel de madurez de seguridad de la información e informática y mantener de forma segura los datos que se tiene dentro de la institución.

Pregunta 2: ¿En qué provincia del Ecuador se encuentra ubicada su empresa?

Según las respuestas obtenidas de las entrevistas aplicadas a los gerentes, se evidenció que mayoritariamente estas empresas se encuentran en las provincias de Pichincha, Guayaquil, Imbabura, Tungurahua y Manabí.

Pregunta 3: ¿Considera importante que las empresas utilicen estructuras para conocer los niveles de madurez de la seguridad de la información?

En los resultados de las entrevistas, se menciona que un modelo para medir el nivel de madurez de los controles de seguridad a la información sí es importante, porque les ayuda a identificar las vulnerabilidades que tienen las empresas y por las cuales pueden sufrir un ciberataque y, con ello, pérdida de información, con estos datos pueden mejorar la seguridad de la información que se almacena dentro de la organización.

Pregunta 4: ¿Utiliza algún modelo, estructura o estrategia para medir el nivel de madurez de seguridad de la información de su empresa?

Con la recolección de la información se evidenció que la mayoría de las empresas seleccionadas utilizan la consultoría externa y la metodología del consultor para medir el nivel de madurez de la información dentro de sus gestiones. Identificando que ninguna entidad participante aplica un modelo de evaluación de madurez de la información.

Pregunta 5: ¿Qué modelo utiliza para medir el nivel de madurez?

Según los datos recolectados de las entrevistas, se identificó que tres empresas utilizan un modelo propio de consultor con la normativa vigente, mientras que una empresa hace uso de la evaluación de los controles aplicables ISO 27001, y, otra empresa no implementa ningún modelo.

Pregunta 6: ¿Qué modelos para la evaluación de nivel de madurez de la seguridad de la información conoce?

Continuando con el análisis de los datos recolectados de la entrevista se evidenció que todas las empresas conocen el modelo Magerit, Controles ISO 27001 para medir el nivel de madurez de la seguridad de la información de las empresas.

Pregunta 7: ¿Cree usted que un modelo para medir el nivel de madurez de la información ayudará a proteger los datos de su empresa?

Tomando de referencia la información recolectada, se observó que los gerentes de las empresas de aseguradoras del Ecuador, están de acuerdo con el desarrollo del modelo para medir el nivel de madurez de la información, debido a que les ayudaría a proteger los datos de su actividad económica y mejorar sus seguridades de protección de la información implementando nuevos controles internos.

Pregunta 8: ¿Estaría dispuesto a utilizar un modelo para medir el nivel de madurez de la información de su empresa?

Los gerentes de las empresas aseguradoras del Ecuador mencionaron que estarían dispuestos a utilizar un modelo para medir el nivel de madurez de la información siempre que no genere demora en los procesos de negocios. Utilizando las mejores prácticas y estándares de seguridad vigentes.

CAPÍTULO II: PROPUESTA

A continuación, el desarrollo de la propuesta que este trabajo pretende entregar.

Fundamentos teóricos aplicados

En la investigación desarrollada por Atencio (2019) se planteó diseñar un sistema de gestión de seguridad de la información basada en la NTP ISO/IEC 27001:2014, para mejorar la integridad, confidencialidad y disponibilidad de los activos de información en la DGIyE de la UNDAC donde se identificó vulnerabilidades y amenazas, y se empleó la metodología de MAGERIT para la gestión de riesgos e implementar los controles de seguridad para reducir los riesgos presentados.

Según Gené (2018), la seguridad de la información es un conjunto de normativas y políticas a seguir para una correcta protección de los datos que tiene una organización, porque es una pieza fundamental para que la empresa lleve sus operaciones sin ningún riesgo y los datos sean manejados de una forma correcta. La seguridad de la información se trata de la identificación, análisis y prevención de los datos y de esta forma encontrar soluciones rápidas y eficientes para su protección.

La seguridad de la información está basada en cuatro etapas fundamentales para una correcta protección de los datos. La disponibilidad es el acceso a la información cuando se requiere, teniendo en cuenta la correcta privacidad y seguridad desde el lugar que se quiera acceder, también se tiene la confidencialidad como una variable que indica que solo podrá ingresar personal con autorización con el fin de evitar que esta información llegue a personas que pretendan hacer mal uso de esta.

La integridad como elemento de gestión es la protección de la información que no sea modificada por personas que no estén autorizadas y que generen errores o fugas de información fuera de la institución. Finalmente, la fase de autenticación procede a verificar que el usuario que intenta ingresar u obtener información pertenezca a la institución o esté autorizado por la misma.

Modelo de la seguridad de la información

Según la investigación desarrollada por García et al. (2018), mencionan que en la actualidad las empresas tratan de proteger su información valiosa para minimizar los riegos de pérdidas de datos y evitar situaciones negativas como son falencias de carácter económico significativo, violación de confidencialidad, perdidas de integridad, entre otros, por lo cual, las grandes empresas han implementado modelos para medir el nivel de

madurez de la información e identificar las fortalezas y vulnerabilidades que se encuentran en la institución, la finalidad es solucionar y evitar posibles fugas de datos susceptibles que provoquen problemas con sus clientes.

El modelo de la seguridad de la información permite a la empresa conocer sus activos y los riesgos que estos presentan. Se pretende cuantificar las vulnerabilidades que se tienen y brindar controles necesarios para contrarrestar estas falencias mediante la estimación de riesgos, para esto, se realizó un análisis donde se resaltó sus fortalezas y vulnerabilidades, con ello se podrá aplicar un control de riesgos a las instituciones.

Normativas para la valoración de la seguridad de la información

- **ISO 27000**

Es un estándar de la familia ISO, en la actualidad es uno de los más utilizados y considerados por entes de regulación nacionales e internacionales, así mismo, ha sido la base de un sin número de organizaciones en Ecuador para fortalecer los sistemas de gestión de la seguridad de la información de cada una de ellas, estos sistemas basados en la ISO 27000 propone diseños a mecanismos más resistentes y confiables para los usuarios. (Ladino et al., 2011)

- **SysAdmin Audit Network Security (SANS)**

Evalúa diversos estándares y normas de configuración en los sistema de una organización, analiza todos los componentes del sistema y controla que todas las normas de configuración del sistema concuerden con las directrices de seguridad adecuados y aceptadas en la industria. (PCI, 2008)

- **NIST 800**

Es el control de seguridad y privacidad para sistemas de información y organizaciones, el cual, permite proteger las operaciones y los activos de la organización, las personas y la nación de un conjunto diversas amenazas, que incluyen ataques hostiles, errores humanos, desastres naturales, daños estructurales (Fuerza de Tarea Conjunta, 2020)

- **PCI 3.0**

Fueron desarrolladas para fomentar y mejorar la seguridad de los datos de las empresas y facilitar la adopción de medidas de seguridad a nivel mundial. Asimismo, proporcionan una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los clientes. (PCI, 2013).

Modelo de madurez propuesto vs modelo COBIT

Como se menciona en la página oficial de ISACA (2019), COBIT es un modelo de madurez enfocado en la evaluación del nivel de madurez por medio de Benchmarking o también llamado punto de referencia que evalúa y analiza los aspectos de otras empresas con el fin de tomar como fundamento para las futuras estrategias de las entidades, siendo un modelo cualitativo. Mientras que el modelo de madurez planteado en el presente trabajo de investigación está basado en evaluar y garantizar la seguridad de la información por medio de un modelo de 24 controles basados en los estándares internacionales como SANS, NIST CF, PCI 3.0 e ISO 27001, los mismos que se dividen en 5 etapas como son: prevenir, etapa detectar, etapa responder, etapa predecir y etapa gestión, priorizando el número de niveles de madurez mediante un mapa de calor que permite enfocar la mejora de la seguridad de los datos en los números en rojo, siendo un enfoque cualitativo que valora la cualidades de los niveles y cuantitativo, puesto que, mediante fórmulas puede identificar los inconvenientes que se presentan en la compañía para que sean resueltas con la implementación de controles de mejora.

Descripción de la propuesta

Modelo para la evaluación del nivel de madurez de seguridad de la información.

Recolección de datos

Se lleva un registro de la empresa, a la cual, se va a valorar el nivel de madurez, en donde se recolecta datos generales de la institución como es el nombre de la empresa, de la misma forma, se identifica los números de contacto de la empresa y el nombre del responsable de quien levantó la información, como también la fecha que se hizo la valoración.

Figura 3

Levantamiento de información general

LEVANTAMIENTO DE INFORMACION GENERAL - COMPAÑÍA X	
EMPRESA*:	
CONTACTO*:	Luis Vallejo
TELÉFONO*:	
CORREO ELECTRÓNICO*:	
ELABORADO POR*:	
FECHA*:	miércoles, 1 de marzo de 2023
*Campos Obligatorios	

Nota: Tomado de Estructura para evaluación de nivel de madurez

La matriz de recolección de datos cuenta con ocho apartados que son indispensables para la valoración, en el primer punto se recolecta la información del Personal Involucrado en la Evaluación donde se realiza un levantamiento de los datos de los usuarios involucrados en la investigación como el nombre y apellidos, empresa a la cual pertenece, el cargo que desempeña dentro de la empresa y el correo electrónico.

Figura 4

Personal involucrado en la empresa

1) Personal Involucrado en la Evaluación					
N°	Nombres	Apellidos	Empresa	Cargo/Funciones	Correo Electrónico
1	*Luis*	*Vallejo*		*Analista de Seguridad de la Información y Tecnologia*	
2					
3					
4					

En el segundo punto se toman los datos de la cantidad de usuarios o la cantidad totales de direcciones IP utilizadas dentro de la red donde se identifica el tipo personal, la cantidad total, el sistema operativo más común que utiliza y las observaciones importantes en esta recolección de la información.

Figura 5

Recolección de la información de las empresas

3) ¿Cuál es la tasa anual de crecimiento de usuarios estimado? Indique porcentualmente.					
	Ejm: 10% anual				
4) ¿Cuántos enlaces de salida a internet en la oficina Principal o Matriz, dispone actualmente y su ancho de banda?					
N°	Nombre ISP	Modalidad	Tipo de conexión	Ancho de Banda Actual(Mbps)	Ancho de Banda Futuro (Mbps)
1					
2					

En el tercer punto se toma la información de tasa anual de crecimiento de usuarios estimado en la institución. De la igual forma, en el cuarto punto se analiza los enlaces de salida a internet en la oficina principal o la matriz y se determina si cuenta con un ancho de banda, estos datos llevan el nombre ISP, modalidad, tipo de conexión que tiene la empresa, el ancho de banda actual y el ancho de banda que planea obtener a futuro.

Figura 6

Información de las extensiones de las empresas

5) Detalle total de oficinas remotas o sucursales con salida directa a Internet o enlaces de datos (indicar por separado para cada sitio):

N°	Nombre Sucursal	Localidad / Ciudad	Número de usuarios o IPs	Actual(Mbps)	Navegan a través de que
1					
2					
3					
4					
5					

6) Cuales son las Áreas Funcionales - Departamentos de la Empresa.

N°	Departamento	Área Funcional	Descripción	Responsable del Área	# de Personas	Servicio Critico
1						
2						
3						

7) Cuales son los Servicios de Tecnología críticos de la Empresa

N°	Servicios de IT	Descripción	Arquitectura Básica	Cantidad de Usuarios	Quien lo Administra	Que áreas lo usan, como	Observaciones
1							
2							
3							
4							
5							

En el quinto apartado se detalla los datos de las oficinas secundarias o sucursales con salida directa a internet o enlaces de datos como es el nombre de la sucursal, la ubicación que se encuentra, el número de usuarios o IPs, La navegación del ancho de banda y la navegación que utiliza. De igual forma en el sexto punto se detalla cuáles son las áreas funcionales dentro de la empresa, aclarando temas como departamento, el área funcional, la descripción del responsable del área a la cual se va a aplicar la investigación, el número de personas que se encuentran en el área y el servicio crítico.

En el séptimo punto se identifican los servicios de tecnología críticos de la empresa como la cobranza, el pago a proveedores, atención al cliente, etc. Aquí se dá una descripción de su arquitectura básica, la cantidad de usuarios que utilizan este proceso o servicio, quien la administra, qué áreas hacen uso y la observación.

De la misma forma se detalla el nivel y las respuestas.

Figura 7

Nivel y respuesta del análisis

RIESGO/NIVEL	Puntuación-Criticidad	RESPUESTAS	Puntuación-Criticidad
5 - Critico	8	0 - No existente	5
4 - Alto	7	1 - Realizado	4
3 - Medio	3	2 - Gestionado	3
2 - Bajo	2	3 - Establecido	2
1 - Muy bajo	1	4 - Predecible	1
		5 - Optimizado	0
	0,5		0,5

Lineamientos de calificación

Los lineamientos que utilizan las empresas para identificar el nivel de madurez de la información son seis, los mismos que son detallados a continuación: el nivel de valoración “optimizado” es el 100% de madurez en los diferentes controles de seguridad debido a que los procesos han sido llevados a niveles óptimos asociados a las mejores prácticas, tomando como base los resultados de la mejora continua, siendo posible así realizar un seguimiento oportuno y medir el cumplimiento en el uso de los procedimientos, así como tomar acciones correctivas o preventivas oportunamente en caso de detectar una falla, a la cual se le realizará un seguimiento para identificar el ataque.

De la misma forma el nivel de valoración “predecible” pertenece al 80% de madurez, en este nivel se desarrolla un seguimiento y se mide el cumplimiento de los procesos. Por su parte, el nivel de valoración “establecido” pertenece al 60% de madurez en donde se encuentra todo debidamente documentado, pero la responsabilidad de la seguridad de la información recae sobre cada usuario y es poco probable que se identifiquen desviaciones a los estándares establecidos.

La etapa de valoración “gestionado” pertenece al 40% de madurez de la información, en la que los procesos se han desarrollado hasta un punto y son utilizados por varias personas para llevar a cabo la misma tarea, incluso cuando no está correctamente documentado. A diferencia de la etapa de valoración “realizado” que tiene un 20% de nivel de maduración, identificando situaciones que necesitan un tratamiento para mejorar sus niveles de evolución en los controles de seguridad; otro ítem a considerar en la calificación es el incumplimiento de las políticas o procesos establecidos en la institución. Finalmente se tiene el nivel de valoración “no existente”, observando que la institución carece totalmente de procesos relacionados con seguridad de la información. Estos planteamientos permiten determinar las falencias que tiene la organización por mejorar en temas del nivel de seguridad, como también las fortalezas de seguridad.

Figura 8

Lineamientos de calificación para el nivel de madurez

Valoración	% de Madurez	Descripción
Optimizado	100%	Los procesos han sido llevados al nivel de mejores prácticas, con base en los resultados de la mejora continua. Es posible hacer un seguimiento y medir el cumplimiento de los procedimientos, así como tomar acciones correctivas o preventivas cuando se detectan fallas y hacer un seguimiento dichas acciones.
Predecible	80%	Es posible hacer un seguimiento y medir el cumplimiento de los procedimientos, aunque no es constante que se tomen acciones correctivas o preventivas.
Establecido	60%	Los procesos se encuentran totalmente documentados pero la responsabilidad del cumplimiento recae en cada individuo y es poco probable que se detecten desviaciones a los estándares establecidos.
Gestionado	40%	Los procesos se han desarrollado hasta un punto en el cual procedimientos similares son utilizados por personas diferentes para llevar a cabo la misma tarea, incluso cuando estos no se encuentran totalmente documentados.
Realizado	20%	Se ha identificado una situación que debe ser tratada y ya se han implementado acciones aun cuando no hay directivas o procesos documentados relacionados con dichas acciones. Otro motivo de esta calificación es el incumplimiento crítico de la política o proceso ya establecido, el cual no es cumplido.
No existente	0%	Carencia total de procesos relacionados con la Seguridad de la información. La organización no ha identificado una situación que debe ser tratada.

Controles de Seguridad y Gestión 24 (CSG24)

El modelo realizado para evaluar la madurez de los controles de seguridad de la información está estructurado en seis niveles, los cuales, cuentan con 24 controles de valoración que ayudan a identificar los puntos donde las empresas presentan debilidades y cuales cumplen a cabalidad todos los requisitos de seguridad. A continuación, se detalla cada uno de los niveles que conforman el modelo de evaluación de madurez, los mismo que permitirán identificar los procesos de la información, evaluación de riesgos, e implementación de controles que se tendrán en cuenta para la valoración del estado actual de la seguridad de los datos de las entidades objetos a estudio. Asimismo, se enumera los controles que se va aplicar el nivel de madurez, identificando que tiene la organización, el riesgo o nivel tiene cinco niveles de puntuación, siendo el puntaje de 1 muy bajo dando entender que es mínimo y el puntaje de cinco es crítico, el cual, evidencia que se tiene problemas en seguridad.

También en la respuesta cuenta con cinco niveles siendo el nivel cero que no tiene una respuesta para solucionar el problema y el nivel 5, donde se encuentra optimizado. De igual

forma, con estas calificaciones se obtiene la puntuación de los controles del nivel de madurez, para sacar el porcentaje de madurez que tiene el control, el porcentaje esperado y, finalmente, el porcentaje total de la brecha del nivel de madurez en los controles de seguridad de la información e informática.

Etapa prevenir

En la etapa de prevención se identificó los controles de inventario de hardware, el inventario de software, configuraciones de seguridad de hardware y software, seguridad de aplicaciones, configuraciones de seguridad para dispositivos de red, control de puertos y servicios, defensa perimetral, protección de Email y Web, defensa de punto final (Endpoints), protección de plataformas móviles, de redes inalámbricas y de datos, endurecimiento de servidores y estaciones de trabajo y el control de acceso físico, las cuales, son valoradas y puntuadas para la identificación de las brechas. En esta etapa se puede prevenir los posibles ataques al robo de la información, identificando las principales falencias que tiene la institución y cuáles son sus fortalezas.

Figura 9

Etapa de prevenir

ETAPA	No	CONTROLES	SE TIENE:	RIESGO/NIVEL	RESPUESTAS	PUNTOS	% MADUREZ	%ESPERADO	%BRECHA
PREVENIR	1	Inventario de Hardware		3		9	1,3%	2,2%	40,0%
	2	Inventario de Software		4		15	2,2%	2,2%	0,0%
	3	Configuraciones de Seguridad de Hardware y Software		4		30	4,3%	4,3%	0,0%
	4	Seguridad de Aplicaciones		5		25	3,6%	3,6%	0,0%
	5	Configuraciones de		4		15	2,2%	2,2%	0,0%
	6	Control de Puertos y Servicios		4		15	2,2%	2,2%	0,0%
	7	Defensa Perimetral		5		65	9,4%	9,4%	0,0%
	8	Protección de Email y Web		5		11	1,6%	5,1%	68,6%
	9	(Endpoints)		5		50	7,2%	7,2%	0,0%
	10	móviles		4		15	2,2%	2,2%	0,0%
	11	Protección de redes		4		13	1,9%	3,6%	48,0%
	12	Protección de Datos		4		55	8,0%	8,0%	0,0%
	13	Endurecimiento de Servidores y Estaciones de trabajo		4		15	2,2%	2,2%	0,0%
	14	Control de acceso físico		4		5	0,7%	3,6%	80,0%

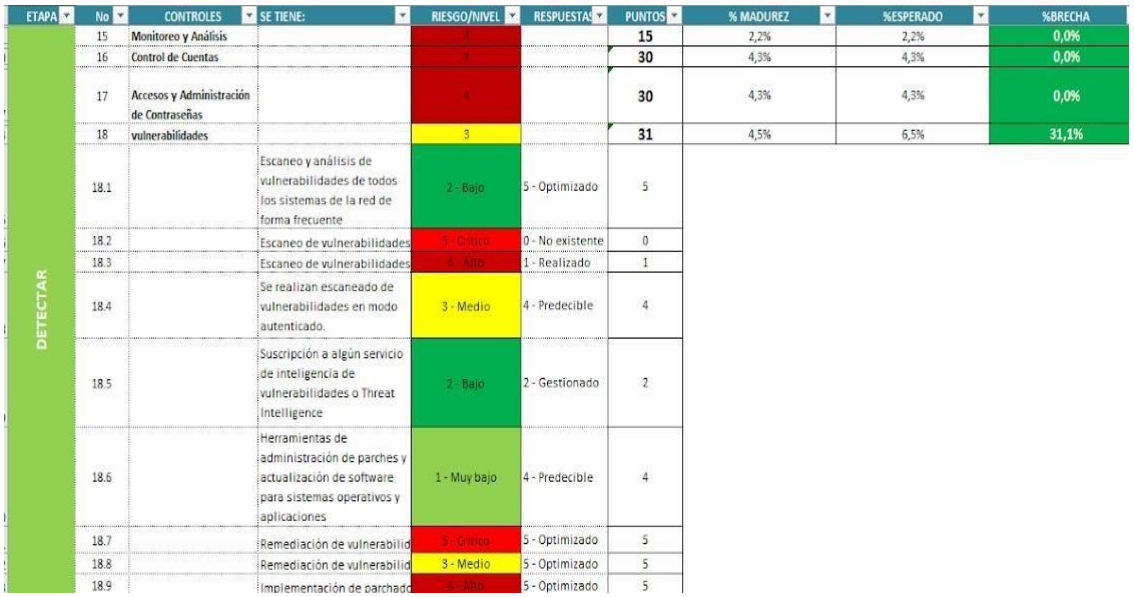
Etapa detectar

En la etapa de detección se identifica los controles de monitoreo y análisis, inspección de cuentas, accesos y administración de contraseñas, el escaneo y remediación de vulnerabilidades que sirven para detectar los posibles ataques cibernéticos que sufre las instituciones en el robo de la información, determinando las brechas que se tiene para

optimizar los niveles de madurez en controles de seguridad de la información en las empresas.

Figura 10

Etapa de detección



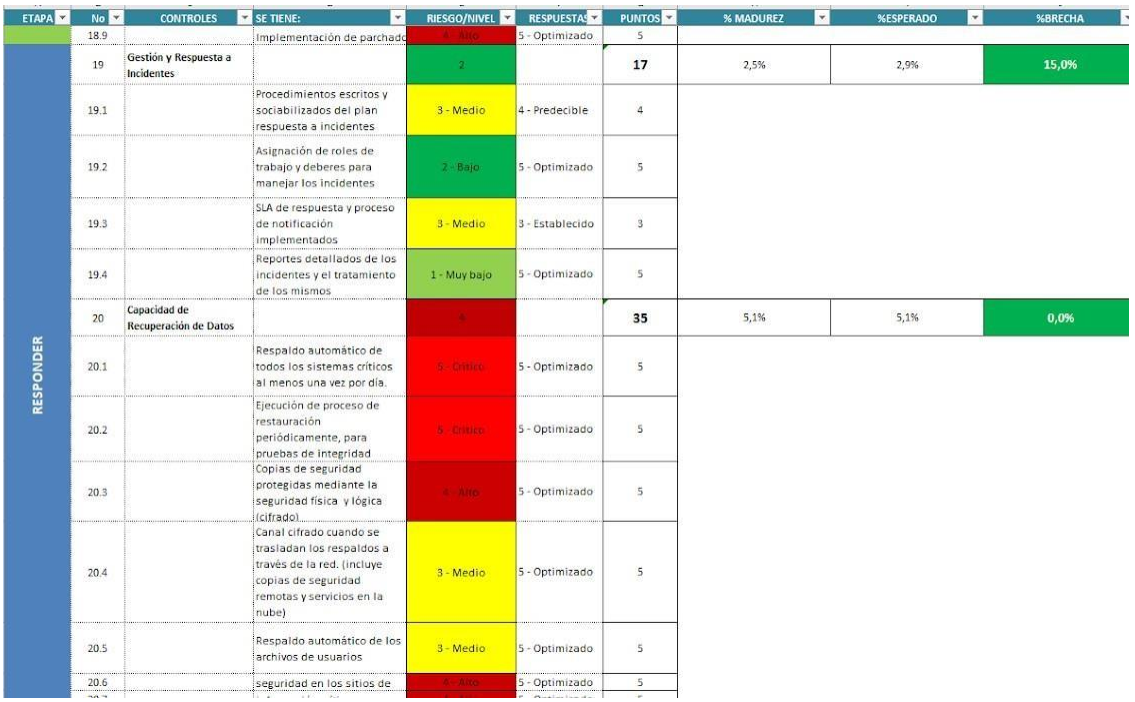
ETAPA	No	CONTROLES	SE TIENE:	RIESGO/NIVEL	RESPUESTA	PUNTOS	% MADUREZ	%ESPERADO	%BRECHA
DETECTAR	15	Monitoreo y Análisis		3		15	2,2%	2,2%	0,0%
	16	Control de Cuentas		4		30	4,3%	4,3%	0,0%
	17	Accesos y Administración de Contraseñas		4		30	4,3%	4,3%	0,0%
	18	vulnerabilidades		3		31	4,5%	6,5%	31,1%
	18.1		Escaneo y análisis de vulnerabilidades de todos los sistemas de la red de forma frecuente	2 - Bajo	5 - Optimizado	5			
	18.2		Escaneo de vulnerabilidades	5 - Crítico	0 - No existente	0			
	18.3		Escaneo de vulnerabilidades	4 - Alto	1 - Realizado	1			
	18.4		Se realizan escaneado de vulnerabilidades en modo autenticado.	3 - Medio	4 - Predecible	4			
	18.5		Suscripción a algún servicio de inteligencia de vulnerabilidades o Threat Intelligence	2 - Bajo	2 - Gestionado	2			
	18.6		Herramientas de administración de parches y actualización de software para sistemas operativos y aplicaciones	1 - Muy bajo	4 - Predecible	4			
	18.7		Remediación de vulnerabilid	5 - Crítico	5 - Optimizado	5			
	18.8		Remediación de vulnerabilid	3 - Medio	5 - Optimizado	5			
	18.9		Implementación de parchado	4 - Alto	5 - Optimizado	5			

Etapa responder

En la etapa de respuesta, se gestiona como tratar los posibles ataques cibernéticos que puede sufrir la institución, se encuentran los controles de gestión y respuesta a incidentes, capacidad de recuperación de datos para responder a los posibles ataques que pretendan vulnerar la información, con la intención de recuperar la máxima información posible que ha sido vulnerada.

Figura 11

Etapa de respuesta



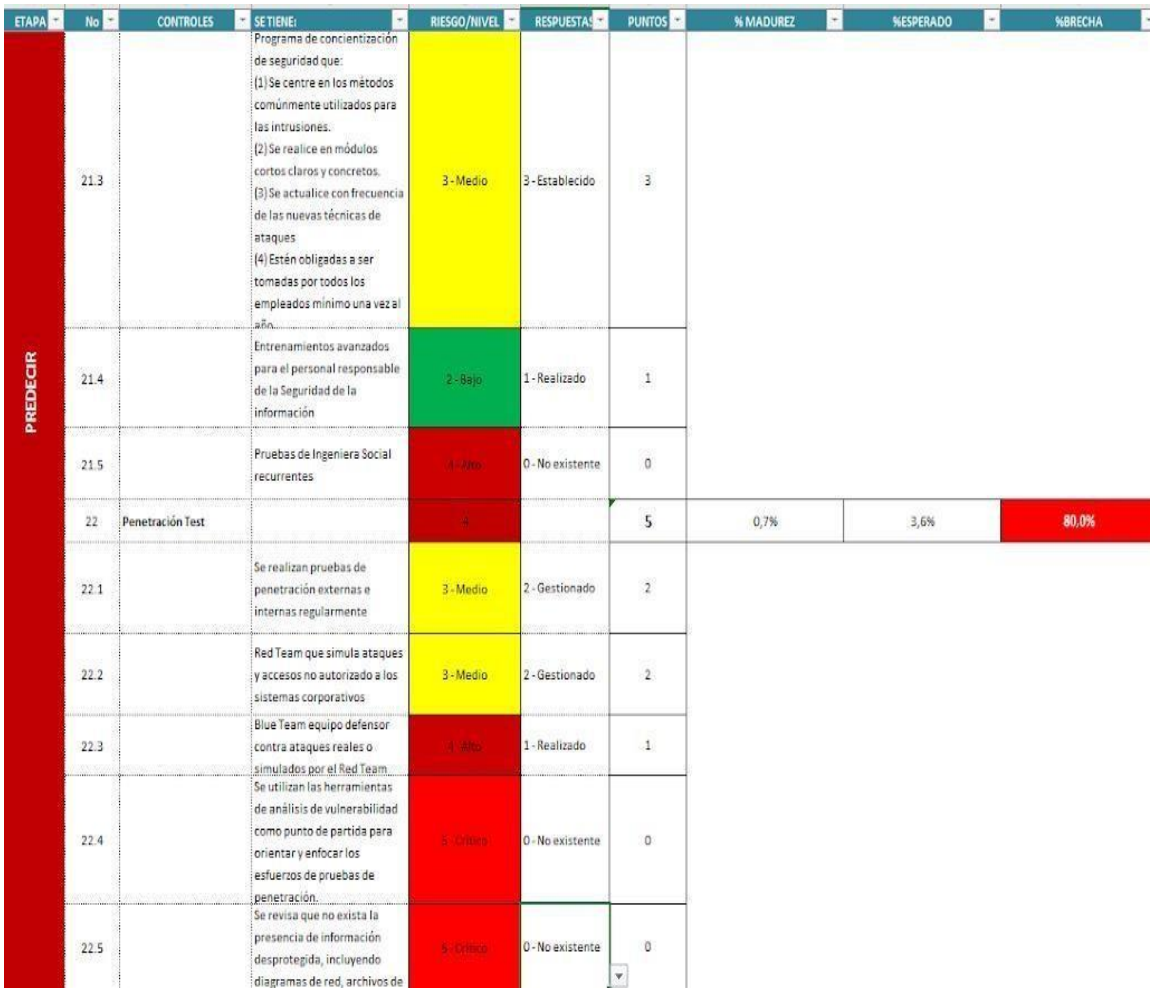
ETAPA	No	CONTROLES	SE TIENE:	RIESGO/NIVEL	RESPUESTAS	PUNTOS	% MADUREZ	%ESPERADO	%BRECHA
	18.9		Implementación de parchado	4 - Alto	5 - Optimizado	5			
RESPONDER	19	Gestión y Respuesta a Incidentes		2		17	2,5%	2,9%	15,0%
	19.1		Procedimientos escritos y sociabilizados del plan respuesta a incidentes	3 - Medio	4 - Predecible	4			
	19.2		Asignación de roles de trabajo y deberes para manejar los incidentes	2 - Bajo	5 - Optimizado	5			
	19.3		SLA de respuesta y proceso de notificación implementados	3 - Medio	3 - Establecido	3			
	19.4		Reportes detallados de los incidentes y el tratamiento de los mismos	1 - Muy bajo	5 - Optimizado	5			
	20	Capacidad de Recuperación de Datos		4		35	5,1%	5,1%	0,0%
	20.1		Respaldo automático de todos los sistemas críticos al menos una vez por día.	5 - Crítico	5 - Optimizado	5			
	20.2		Ejecución de proceso de restauración periódicamente, para pruebas de integridad	5 - Crítico	5 - Optimizado	5			
	20.3		Copias de seguridad protegidas mediante la seguridad física y lógica (cifrado)	4 - Alto	5 - Optimizado	5			
	20.4		Canal cifrado cuando se trasladan los respaldos a través de la red. (incluye copias de seguridad remotas y servicios en la nube)	3 - Medio	5 - Optimizado	5			
	20.5		Respaldo automático de los archivos de usuarios	3 - Medio	5 - Optimizado	5			
	20.6		seguridad en los sitios de	4 - Alto	5 - Optimizado	5			

Etapa predecir

En la etapa de predicción se identifican los controles de entrenamiento a usuarios donde se detecta y evalúa las debilidades de conocimiento de seguridad de los empleados, la capacidad de respuesta ante un ataque, recomendando realizar entrenamientos para prevenir estos posibles ataques, así mismo se tiene el control de penetración Test, en el cual, se realiza pruebas de penetración externa e interna regularmente. La red Team para simular los posibles ataques, el Team azul que es el defensor antes los ataques a las instituciones, también se utilizan las herramientas de identificación de vulnerabilidades y se revisa que no exista información desprotegida que puede ser vulnerada.

Figura 12

Etapa de predicción



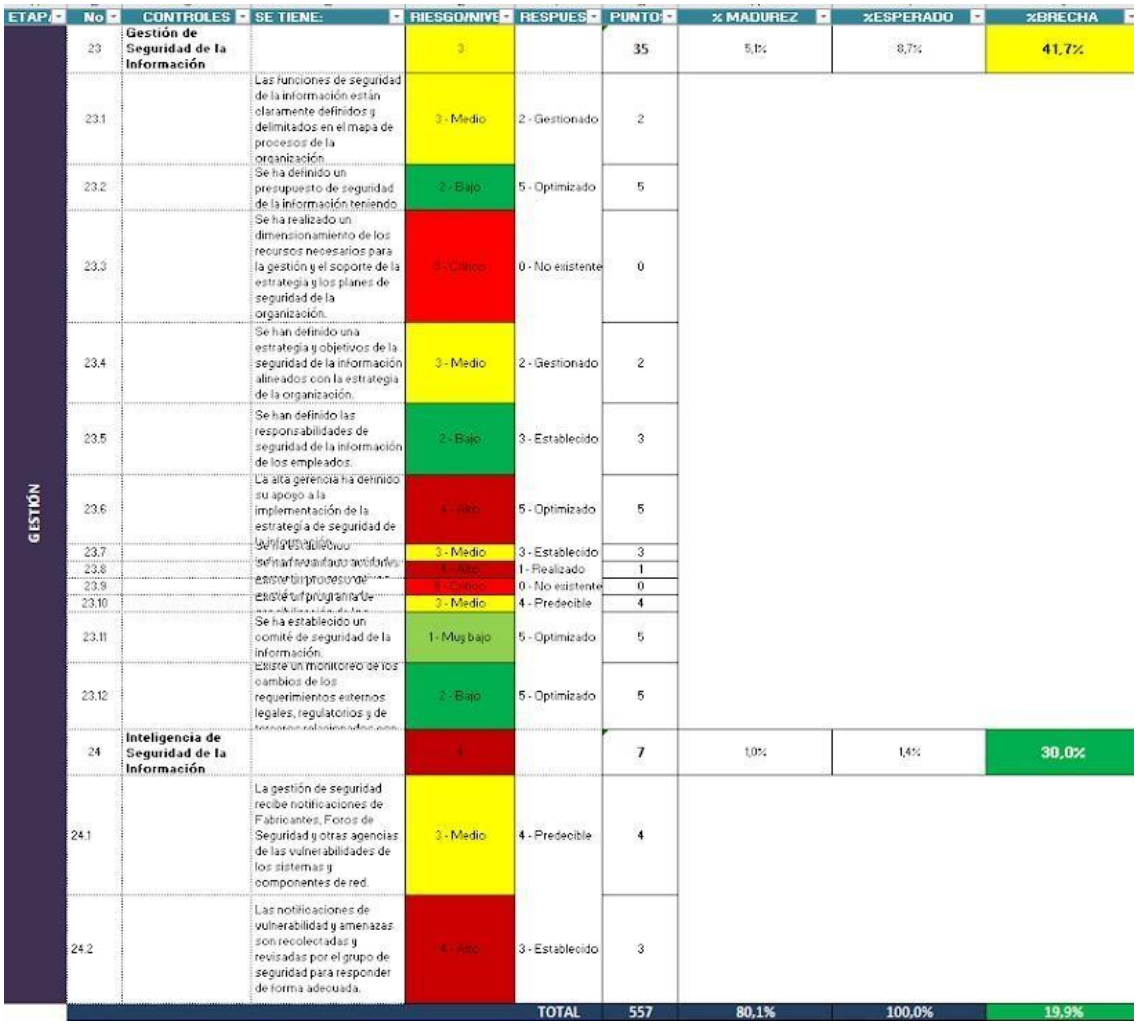
ETAPA	No	CONTROLES	SE TIENE:	RIESGO/NIVEL	RESPUESTAS	PUNTOS	% MADUREZ	%ESPERADO	%BRECHA
PREDECIR	21.3		Programa de concientización de seguridad que: (1) Se centre en los métodos comúnmente utilizados para las intrusiones. (2) Se realice en módulos cortos claros y concretos. (3) Se actualice con frecuencia de las nuevas técnicas de ataques (4) Estén obligadas a ser tomadas por todos los empleados mínimo una vez al año.	3 - Medio	3 - Establecido	3			
	21.4		Entrenamientos avanzados para el personal responsable de la Seguridad de la información	2 - Bajo	1 - Realizado	1			
	21.5		Pruebas de Ingeniera Social recurrentes	4 - Alto	0 - No existente	0			
	22	Penetración Test		4		5	0,7%	3,6%	80,0%
	22.1		Se realizan pruebas de penetración externas e internas regularmente	3 - Medio	2 - Gestionado	2			
	22.2		Red Team que simula ataques y accesos no autorizado a los sistemas corporativos	3 - Medio	2 - Gestionado	2			
	22.3		Blue Team equipo defensor contra ataques reales o simulados por el Red Team.	4 - Alto	1 - Realizado	1			
	22.4		Se utilizan las herramientas de análisis de vulnerabilidad como punto de partida para orientar y enfocar los esfuerzos de pruebas de penetración.	5 - Crítico	0 - No existente	0			
	22.5		Se revisa que no exista la presencia de información desprotegida, incluyendo diagramas de red, archivos de	5 - Crítico	0 - No existente	0			

Etapa gestión

En la etapa de gestión se tiene los controles de administración de seguridad de la información, en la cual, se identifica las funciones de seguridad de la información que deben estar claramente definidas y delimitadas en el mapa de procesos de la organización, también se define las estrategias para proteger la información, estableciendo una competente seguridad de datos, de la misma forma, se tiene el control de inteligencia para desarrollar la gestión de seguridad recibiendo notificación de las vulnerabilidades y amenazas que tiene la organización, con el objetivo de saber cómo responder ante un posible ataque cibernético.

Figura 13

Etapa de gestión



ETAPA	No	CONTROLES	SE TIENE:	RIESGO/NIVE	RESPUES	PUNTO	% MADUREZ	%ESPERADO	%BRECHA
GESTIÓN	23	**Gestión de Seguridad de la Información**		3		35	5,1%	8,7%	41,7%
	23.1		Las funciones de seguridad de la información están claramente definidos y delimitados en el mapa de procesos de la organización.	3 - Medio	2 - Gestionado	2			
	23.2		Se ha definido un presupuesto de seguridad de la información teniendo	2 - Bajo	5 - Optimizado	5			
	23.3		Se ha realizado un dimensionamiento de los recursos necesarios para la gestión y el soporte de la estrategia y los planes de seguridad de la organización.	5 - Crítico	0 - No existente	0			
	23.4		Se han definido una estrategia y objetivos de la seguridad de la información alineados con la estrategia de la organización.	3 - Medio	2 - Gestionado	2			
	23.5		Se han definido las responsabilidades de seguridad de la información de los empleados	2 - Bajo	3 - Establecido	3			
	23.6		La alta gerencia ha definido su apoyo a la implementación de la estrategia de seguridad de	4 - Alto	5 - Optimizado	5			
	23.7			3 - Medio	3 - Establecido	3			
	23.8			4 - Alto	1 - Realizado	1			
	23.9			5 - Crítico	0 - No existente	0			
	23.10			3 - Medio	4 - Predecible	4			
	23.11		Se ha establecido un comité de seguridad de la información.	1 - Muy bajo	5 - Optimizado	5			
	23.12		Existe un monitoreo de los cambios de los requerimientos externos legales, regulatorios y de	2 - Bajo	5 - Optimizado	5			
	24	**Inteligencia de Seguridad de la Información**		4		7	1,0%	1,4%	30,0%
	24.1		La gestión de seguridad recibe notificaciones de Fabricantes, Foros de Seguridad y otras agencias de las vulnerabilidades de los sistemas y componentes de red.	3 - Medio	4 - Predecible	4			
	24.2		Las notificaciones de vulnerabilidad y amenazas son recolectadas y revisadas por el grupo de seguridad para responder de forma adecuada.	4 - Alto	3 - Establecido	3			
					TOTAL	557	80,1%	100,0%	19,9%

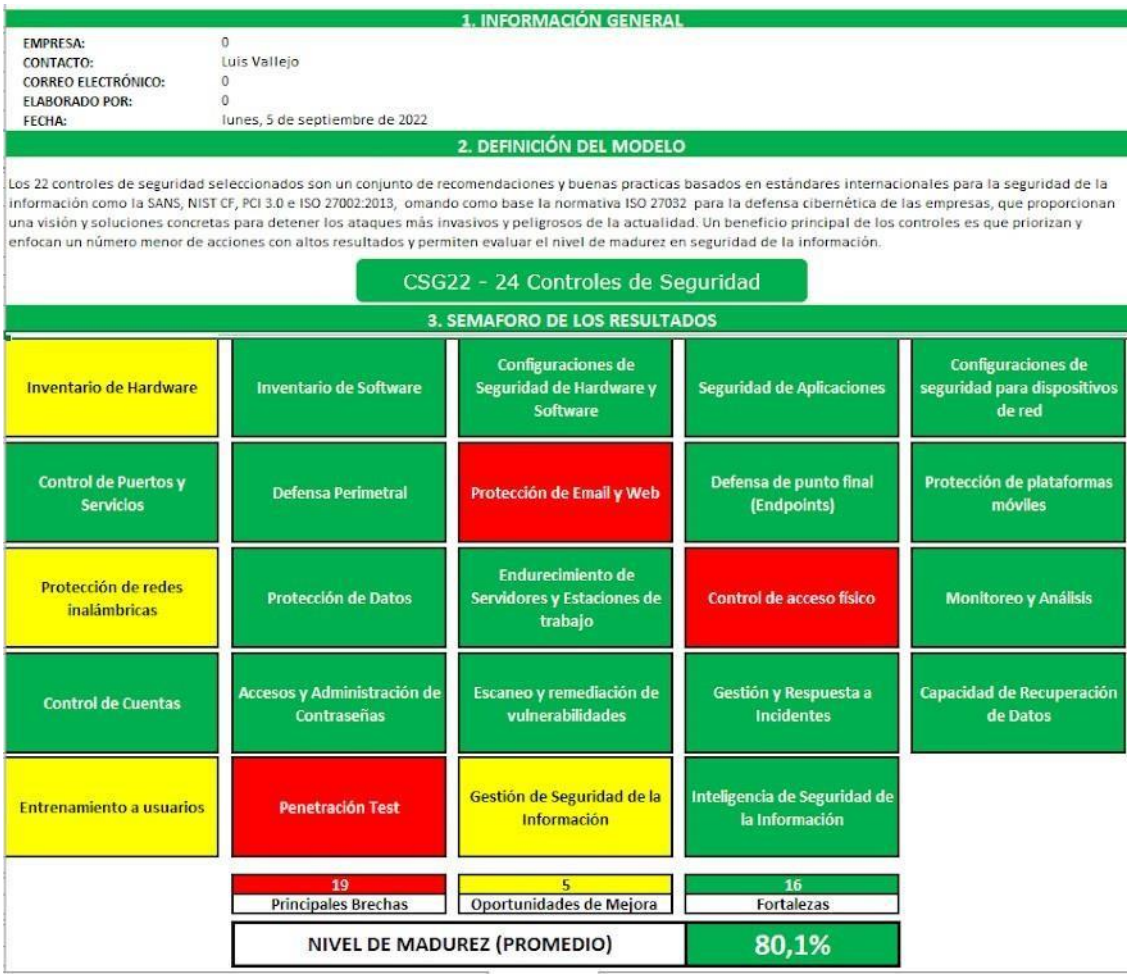
Resultados de la evaluación

Siguiendo con la investigación, en el modelo de evaluación de la madurez se muestran los resultados de evaluación en un mapa de calor donde se puede identificar el nivel de madurez de cada control de seguridad identificando las principales brechas de la empresa, las cuales, se tiene que trabajar para mejorar, asimismo las oportunidades de mejora y las fortalezas que tiene la entidad. Finalmente se obtiene el promedio del nivel de madurez general de la compañía. Los 22 controles de seguridad seleccionados son un conjunto de recomendaciones y buenas prácticas basados en estándares internacionales para la seguridad de la información como la SANS, NIST CF, PCI 3.0 e ISO 27002:2013, tomando como base la normativa ISO 27032 para la defensa cibernética de las empresas, que proporcionan una visión y soluciones concretas para detener los ataques más invasivos y peligrosos de la actualidad. Un beneficio principal de los controles es que priorizan y

enfocan un número menor de acciones con altos resultados y permiten evaluar el nivel de madurez en seguridad de datos.

Figura 14

Mapa de calor de los resultados obtenidos con la valoración

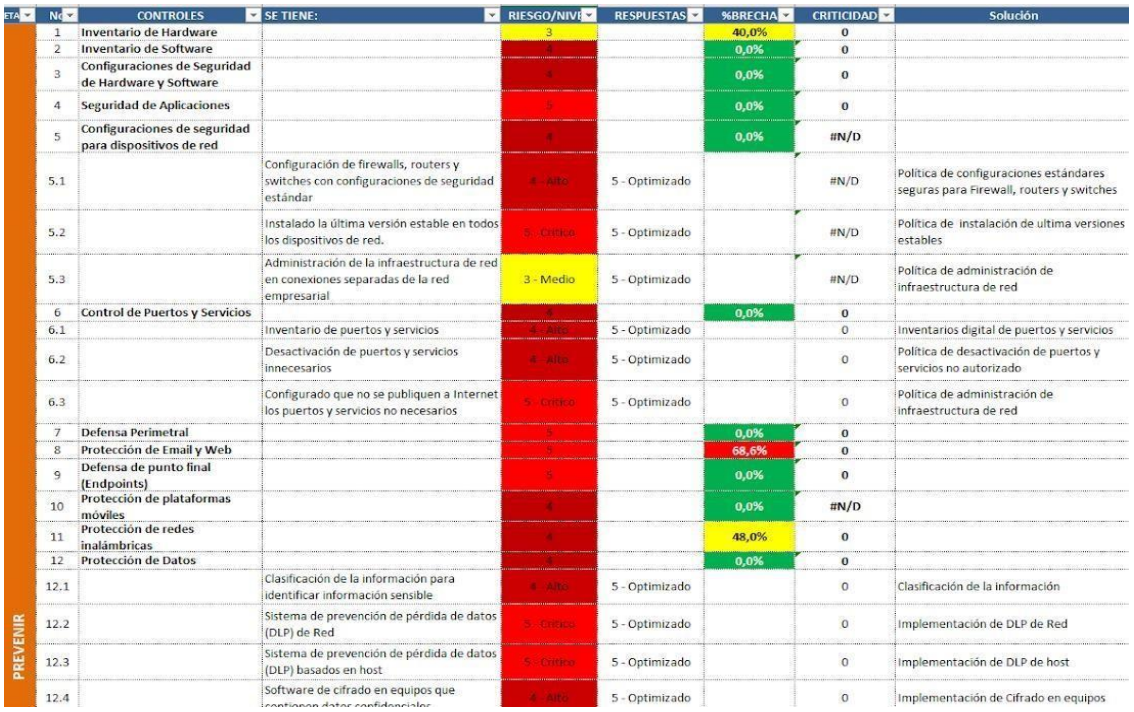


Soluciones para implementarse

Según los resultados obtenidos mediante la recolección y análisis de datos de los 24 controles establecidos en el modelo, se identifica las falencias existentes en las empresas con la finalidad de dar solución a los controles que presentan vulnerabilidades y de esta forma se optimizará la seguridad de la información, esta matriz identifica las posibles soluciones por medio del riesgo que presenta el nivel de madurez.

Figura 15

Resultados de controles 1 al 12.4



ETA	No	CONTROLES	SE TIENE:	RIESGO/NIVE	RESPUESTAS	%BRECHA	CRITICIDAD	Solución
	1	Inventario de Hardware		3		40,0%	0	
	2	Inventario de Software		5		0,0%	0	
	3	Configuraciones de Seguridad de Hardware y Software		4		0,0%	0	
	4	Seguridad de Aplicaciones		5		0,0%	0	
	5	Configuraciones de seguridad para dispositivos de red		4		0,0%	#N/D	
	5.1		Configuración de firewalls, routers y switches con configuraciones de seguridad estándar	4 - Alto	5 - Optimizado		#N/D	Política de configuraciones estándares seguras para Firewall, routers y switches
	5.2		Instalado la última versión estable en todos los dispositivos de red.	5 - Crítico	5 - Optimizado		#N/D	Política de instalación de ultima versiones estables
	5.3		Administración de la infraestructura de red en conexiones separadas de la red empresarial	3 - Medio	5 - Optimizado		#N/D	Política de administración de infraestructura de red
	6	Control de Puertos y Servicios		4		0,0%	0	
	6.1		Inventario de puertos y servicios	4 - Alto	5 - Optimizado		0	Inventarios digital de puertos y servicios
	6.2		Desactivación de puertos y servicios innecesarios	4 - Alto	5 - Optimizado		0	Política de desactivación de puertos y servicios no autorizado
	6.3		Configurado que no se publiquen a Internet los puertos y servicios no necesarios	5 - Crítico	5 - Optimizado		0	Política de administración de infraestructura de red
	7	Defensa Perimetral		5		0,0%	0	
	8	Protección de Email y Web		1		68,6%	0	
	9	Defensa de punto final (Endpoints)		5		0,0%	0	
	10	Protección de plataformas móviles		4		0,0%	#N/D	
	11	Protección de redes inalámbricas		4		48,0%	0	
	12	Protección de Datos		1		0,0%	0	
PREVENIR	12.1		Clasificación de la información para identificar información sensible	4 - Alto	5 - Optimizado		0	Clasificación de la información
PREVENIR	12.2		Sistema de prevención de pérdida de datos (DLP) de Red	5 - Crítico	5 - Optimizado		0	Implementación de DLP de Red
PREVENIR	12.3		Sistema de prevención de pérdida de datos (DLP) basados en host	5 - Crítico	5 - Optimizado		0	Implementación de DLP de host
PREVENIR	12.4		Software de cifrado en equipos que contienen datos confidenciales	4 - Alto	5 - Optimizado		0	Implementación de Cifrado en equipos

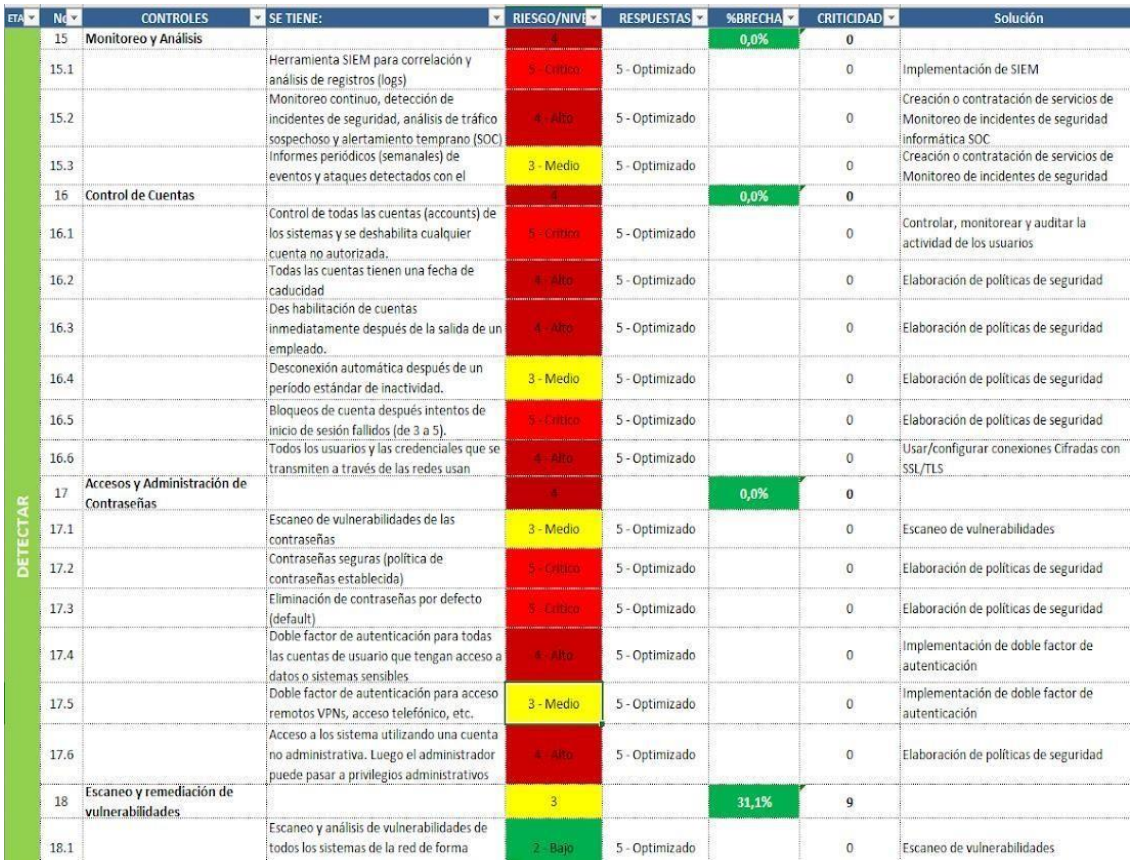
Figura 16

Resultados de controles 12 al 14.5

	12	Protección de Datos		4		0,0%	0	
PREVENIR	12.1		Clasificación de la información para identificar información sensible	4 - Alto	5 - Optimizado		0	Clasificación de la información
PREVENIR	12.2		Sistema de prevención de pérdida de datos (DLP) de Red	5 - Crítico	5 - Optimizado		0	Implementación de DLP de Red
PREVENIR	12.3		Sistema de prevención de pérdida de datos (DLP) basados en host	5 - Crítico	5 - Optimizado		0	Implementación de DLP de host
PREVENIR	12.4		Software de cifrado en equipos que contienen datos confidenciales	4 - Alto	5 - Optimizado		0	Implementación de Cifrado en equipos
PREVENIR	12.5		Bloqueado el acceso a sitios web y aplicaciones conocidas para la transferencia de archivos. (ejemplo:	4 - Alto	5 - Optimizado		0	Política/Configuración de bloqueos
PREVENIR	12.6		Enmascaramiento de datos dinámicos (dynamic data masking)	4 - Alto	5 - Optimizado		0	Implementación de Enmascaramiento de datos dinámicos (dynamic data masking)
PREVENIR	12.7		Comunicación de información confidencial sobre redes menos confiables cifrada	4 - Alto	5 - Optimizado		0	Usar/configurar conexiones Cifradas con SSL/TLS
PREVENIR	12.8		Encriptación de correo saliente que contien	3 - Medio	5 - Optimizado		0	Implementación de Encriptación de correo saliente
PREVENIR	12.9		Los datos que son archivados (Data Archiving) o los sistema a los que no se accede regularmente son apagados hasta	3 - Medio	5 - Optimizado		0	Política de desactivación de hardware
PREVENIR	12.10		Firewall de database DBF	5 - Crítico	5 - Optimizado		0	Implementación de firewall de database
PREVENIR	12.11		Auditoria y logs de accesos a las bases de da	5 - Crítico	5 - Optimizado		0	Implementación de auditorias de database
	13	Endurecimiento de Servidores y Estaciones de trabajo		4		0,0%	0	
	14	Control de acceso físico		4		80,0%	0	
	14.1		Control de acceso al Data Center del personal autorizado con solo los elementos necesarios para desarrollar sus labores.	5 - Crítico	5 - Optimizado		0	Elaboración de políticas de seguridad
	14.2		Implementado un circuito de cámaras de vigilancia con almacenamiento de video	3 - Medio	5 - Optimizado		0	Implementación de cámaras de seguridad
	14.4		Se debe llevar un registro firmado del acceso al Data Center	4 - Alto	5 - Optimizado		0	Elaboración de políticas de seguridad
	14.5		Control de acceso con autenticación de doble factor al Data Center (biométricos, llaves, tarjetas, etc.)	4 - Alto	5 - Optimizado		0	Implementación de biométricos
			Control de acceso con autenticación de					

Figura 17

Resultados de controles 15 al 18.1



ETA	No	CONTROLES	SE TIENE:	RIESGO/NIVE	RESPUESTAS	%BRECHA	CRITICIDAD	Solución
DETECTAR	15	Monitoreo y Análisis		4		0,0%	0	
	15.1		Herramienta SIEM para correlación y análisis de registros (logs)	5 - Crítico	5 - Optimizado		0	Implementación de SIEM
	15.2		Monitoreo continuo, detección de incidentes de seguridad, análisis de tráfico sospechoso y alertamiento temprano (SOC)	4 - Alto	5 - Optimizado		0	Creación o contratación de servicios de Monitoreo de incidentes de seguridad informática SOC
	15.3		Informes periódicos (semanales) de eventos y ataques detectados con el	3 - Medio	5 - Optimizado		0	Creación o contratación de servicios de Monitoreo de incidentes de seguridad
	16	Control de Cuentas		4		0,0%	0	
	16.1		Control de todas las cuentas (accounts) de los sistemas y se deshabilita cualquier cuenta no autorizada.	5 - Crítico	5 - Optimizado		0	Controlar, monitorear y auditar la actividad de los usuarios
	16.2		Todas las cuentas tienen una fecha de caducidad	4 - Alto	5 - Optimizado		0	Elaboración de políticas de seguridad
	16.3		Des habilitación de cuentas inmediatamente después de la salida de un empleado.	4 - Alto	5 - Optimizado		0	Elaboración de políticas de seguridad
	16.4		Desconexión automática después de un período estándar de inactividad.	3 - Medio	5 - Optimizado		0	Elaboración de políticas de seguridad
	16.5		Bloqueos de cuenta después intentos de inicio de sesión fallidos (de 3 a 5).	5 - Crítico	5 - Optimizado		0	Elaboración de políticas de seguridad
	16.6		Todos los usuarios y las credenciales que se transmiten a través de las redes usan	4 - Alto	5 - Optimizado		0	Usar/configurar conexiones Cifradas con SSL/TLS
	17	Accesos y Administración de Contraseñas		4		0,0%	0	
	17.1		Escaneo de vulnerabilidades de las contraseñas	3 - Medio	5 - Optimizado		0	Escaneo de vulnerabilidades
	17.2		Contraseñas seguras (política de contraseñas establecida)	5 - Crítico	5 - Optimizado		0	Elaboración de políticas de seguridad
	17.3		Eliminación de contraseñas por defecto (default)	5 - Crítico	5 - Optimizado		0	Elaboración de políticas de seguridad
	17.4		Doble factor de autenticación para todas las cuentas de usuario que tengan acceso a datos o sistemas sensibles	4 - Alto	5 - Optimizado		0	Implementación de doble factor de autenticación
	17.5		Doble factor de autenticación para acceso remotos VPNs, acceso telefónico, etc.	3 - Medio	5 - Optimizado		0	Implementación de doble factor de autenticación
	17.6		Acceso a los sistema utilizando una cuenta no administrativa. Luego el administrador puede pasar a privilegios administrativos	4 - Alto	5 - Optimizado		0	Elaboración de políticas de seguridad
	18	Escaneo y remediación de vulnerabilidades		3		31,1%	9	
	18.1		Escaneo y análisis de vulnerabilidades de todos los sistemas de la red de forma	2 - Bajo	5 - Optimizado		0	Escaneo de vulnerabilidades

Figura 18

Resultados de controles 18 al 18.9

ETA	No	CONTROLES	SE TIENE:	RIESGO/NIVE	RESPUESTAS	%BRECHA	CRITICIDAD	Solución
	18	Escaneo y remediación de vulnerabilidades		3		31,1%	9	
	18.1		Escaneo y análisis de vulnerabilidades de todos los sistemas de la red de forma frecuente	2 - Bajo	5 - Optimizado		0	Escaneo de vulnerabilidades
	18.2		Escaneo de vulnerabilidades a las bases de d	5 - Crítico	0 - No existente		40	Escaneo de vulnerabilidades
	18.3		Escaneo de vulnerabilidades en servidores D	4 - Alto	1 - Realizado		28	Escaneo de vulnerabilidades
	18.4		Se realizan escaneado de vulnerabilidades en modo autenticado.	3 - Medio	4 - Predecible		3	Escaneo de vulnerabilidades
	18.5		Suscripción a algún servicio de inteligencia de vulnerabilidades o Threat Intelligence	2 - Bajo	2 - Gestionado		6	Suscripción a servicios de inteligencia de vulnerabilidades o Threat Intelligence
	18.6		Herramientas de administración de parches y actualización de software para sistemas operativos y aplicaciones	1 - Muy bajo	4 - Predecible		1	Implementación de gestión y distribución de parches
	18.7		Remediación de vulnerabilidades nivel 4 y 5	5 - Crítico	5 - Optimizado		0	Ejecución de remediación de vulnerabilidades
	18.8		Remediación de vulnerabilidades nivel 2 y 3	3 - Medio	5 - Optimizado		0	Ejecución de remediación de vulnerabilidades
	18.9		Parchado virtual para remediación inmedia	4 - Alto	5 - Optimizado		0	Implementación de parchado virtual

Figura 19

Resultados de controles 18.9 al 20.7

ETA	No	CONTROLES	SE TIENE:	RIESGO/NIVE	RESPUESTAS	%BRECHA	CRITICIDAD	Solución
	18.9		Parchado virtual para remediación inmedia	4 - Alto	5 - Optimizado		0	Implementación de parchado virtual
RESPONDER	19	Gestión y Respuesta a Incidentes		2		15,0%	2	
	19.1		Procedimientos escritos y sociabilizados del plan respuesta a incidentes	3 - Medio	4 - Predecible		3	Elaboración de Planes de Remediación y respuesta de incidentes
	19.2		Asignación de roles de trabajo y deberes para manejar los incidentes	2 - Bajo	5 - Optimizado		0	Elaboración de Planes de Remediación y respuesta de incidentes
	19.3		SLA de respuesta y proceso de notificación implementados	3 - Medio	3 - Establecido		6	Elaboración de Planes de Remediación y respuesta de incidentes
	19.4		Reportes detallados de los incidentes y el tratamiento de los mismos	1 - Muy bajo	5 - Optimizado		0	Elaboración de Planes de Remediación y respuesta de incidentes
	20	Capacidad de Recuperación de Datos		4		0,0%	0	
	20.1		Respaldo automático de todos los sistemas críticos al menos una vez por día.	5 - Crítico	5 - Optimizado		0	Implementación de solución de respaldo
	20.2		Ejecución de proceso de restauración periódicamente, para pruebas de integridad	5 - Crítico	5 - Optimizado		0	Elaboración de políticas de respaldo
	20.3		Copias de seguridad protegidas mediante la seguridad física y lógica (cifrado)	4 - Alto	5 - Optimizado		0	Implementación de solución de respaldo
	20.4		Canal cifrado cuando se trasladan los respaldos a través de la red. (incluye copias de seguridad remotas y servicios en la nube)	3 - Medio	5 - Optimizado		0	Implementación de solución de respaldo
	20.5		Respaldo automático de los archivos de usuarios	3 - Medio	5 - Optimizado		0	Implementación de solución de respaldo
	20.6		Mismas consideraciones de seguridad en los sitios de contingencia (site alternos)	4 - Alto	5 - Optimizado		0	Elaboración de políticas de respaldo
	20.7		Todos los respaldos de información críticos almacenados en otra ubicación física	4 - Alto	5 - Optimizado		0	Elaboración de políticas de respaldo

Figura 20

Resultados de controles 21 al 12.5

ETA	No	CONTROLES	SE TIENE:	RIESGO/NIVE	RESPUESTAS	%BRECHA	CRITICIDAD	Solución
PREDECIR	21	Entrenamiento a usuarios		2		44,0%	10	
	21.1		Evaluación y detección de debilidades de conocimiento de seguridad de los empleados	3 - Medio	5 - Optimizado		0	Evaluación/Capacitación de conocimiento de seguridad
	21.2		Capacitaciones para mejorar habilidades en seguridades. En base al análisis anterior	2 - Bajo	5 - Optimizado		0	Evaluación/Capacitación de conocimiento de seguridad
	21.3		Programa de concientización de seguridad que: (1) Se centre en los métodos comúnmente utilizados para las intrusiones. (2) Se realice en módulos cortos claros y concretos. (3) Se actualice con frecuencia de las nuevas técnicas de ataques (4) Estén obligadas a ser tomadas por	3 - Medio	3 - Establecido		6	Evaluación/Capacitación de conocimiento de seguridad
	21.4		Entrenamientos avanzados para el personal responsable de la Seguridad de la información	2 - Bajo	1 - Realizado		8	Evaluación/Capacitación de conocimiento de seguridad
	21.5		Pruebas de Ingeniera Social recurrentes	4 - Alto	0 - No existente		35	Realizar/Contratar pruebas de Ingeniera Social
	22	Penetración Test		5		80,0%	25	
	22.1		Se realizan pruebas de penetración externas e internas regularmente	3 - Medio	2 - Gestionado		9	Ejecución pruebas de penetración
	22.2		Red Team que simula ataques y accesos no autorizado a los sistemas corporativos	3 - Medio	2 - Gestionado		9	Creación de Red Team
	22.3		Blue Team equipo defensor contra ataques reales o simulados por el Red Team	4 - Alto	1 - Realizado		28	Creación de Blue Team
	22.4		Se utilizan las herramientas de análisis de vulnerabilidad como punto de partida para orientar y enfocar los esfuerzos de pruebas de penetración.	5 - Crítico	0 - No existente		40	Ejecución pruebas de penetración
	22.5		Se revisa que no exista la presencia de información desprotegida, incluyendo diagramas de red, archivos de configuración, informes de prueba de penetración más antiguos, correos electrónicos o documentos que contengan	5 - Crítico	0 - No existente		40	Elaboración de políticas de seguridad

Figura 21

Resultados de controles 23 al 24.2

ETA	No	CONTROLES	SE TIENE:	RIESGO/NIVE	RESPUESTAS	%BRECHA	CRITICIDAD	Solución
GESTIÓN	23	Gestión de Seguridad de la Información		4		41,7%	23	
	23.1		Las funciones de seguridad de la información están claramente definidos y	4 - Alto	3 - Establecido	3	14	
	23.2		Se ha definido un presupuesto de seguridad de la información teniendo en cuenta los	4 - Alto	1 - Realizado	1	28	
	23.3		Se ha realizado un dimensionamiento de los recursos necesarios para la gestión y el	4 - Alto	2 - Gestionado	2	21	
	23.4		Se han definido una estrategia y objetivos de la seguridad de la información alineados	4 - Alto	1 - Realizado	1	28	
	23.5		Se han definido las responsabilidades de seguridad de la información de los	4 - Alto	3 - Establecido	3	14	
	23.6		La alta gerencia ha definido su apoyo a la implementación de la estrategia de	4 - Alto	1 - Realizado	1	28	
	23.7		Se ha establecido indicadores de seguridad y se revisan periodicamente.	4 - Alto	1 - Realizado	1	28	
	23.8		Se han levantado acciones correctivas y preventivas para mitigar debilidades de seguridad de la información	4 - Alto	1 - Realizado	1	28	
	23.9		Existe un proceso de gestión de riesgos de seguridad de la información y es	4 - Alto	1 - Realizado	1	28	
	23.10		Existe un programa de sensibilización de	4 - Alto	1 - Realizado	1	28	
	23.11		Se ha establecido un comité de seguridad de la información.	4 - Alto	4 - Predecible	4	7	
	23.12		Existe un monitoreo de los cambios de los requerimientos externos legales,	4 - Alto	2 - Gestionado	2	21	
	24	Inteligencia de Seguridad de la Información		4		30,0%	14	
	24.1		La gestión de seguridad recibe notificaciones de Fabricantes, Foros de Seguridad y otras agencias de las	4 - Alto	3 - Establecido	3	14	
	24.2		Las notificaciones de vulnerabilidad y amenazas son recolectadas y revisadas por el grupo de seguridad para responder de forma adecuada.	4 - Alto	3 - Establecido	3	14	

Normativas para implementar

Según los 24 controladores establecidos para el desarrollo del modelo para la evaluación del nivel de madurez, se establecerán objetivos que deberán ser implementados mediante la estructura desarrollada, en base a las mejores prácticas de seguridad y estrategias internacionales como son: SANS 6.1, NIST CF, PCI 3.0 e ISO. El desarrollo del presente modelo se enfoca principalmente en la norma internacional ISO 27032 con el fin de prevenir posibles ataques cibernéticos y pérdidas de información.

Figura 22

Objetivos por controles

CONTROLES	OBJETIVO	NORMATIVA				%BRECHA
		SANS 6.1	NIST CF	PCI 3.0	ISO	
Inventario de Hardware	Administración activa que permita conocer e inventariar solo los dispositivos autorizados que forman parte o deben pertenecer a la red, y bloquear el acceso al resto.	Control 1	ID-AM	2.4	A.8.1.1 A.9.1.2 A.13.1.1	40,0%
Inventario de Software	Administración activa que permita conocer e inventariar todo el software de la red, no solo el instalado, si no el que se puede ejecutar	Control 2	ID-AM		A.12.5.1 A.12.6.2	0,0%
Configuraciones de Seguridad de Hardware y Software	Establecer, implementar, y administrar configuraciones seguras usando una configuración rigurosa y un proceso de control de cambios que permita prevenir ataques.	Control 3	PR-IP	2.2 2.3 6.2 11.5	A.14.2.4 A.14.2.8 A.18.2.3	0,0%
Seguridad de Aplicaciones	Gestionar el ciclo de vida de todas las aplicaciones desarrolladas por la empresa, con el fin de prevenir, detectar, y corregir brechas de seguridad	Control 18	PR-IP	6.3 6.5-6.7	A.3.4.5 A.12.1.4 A.14.2.1 A.14.2.6 - A.14.2.8	0,0%
Configuraciones de seguridad para dispositivos de red	Establecer, implementar y administrar activamente (rastreo/reportes/corrección) las configuraciones seguras de los dispositivos de red, usando gestión de configuraciones seguras y un proceso de control de cambios.	Control 11	PR-IP	1.1-1.2 2.2 6.2	A.9.1.2 A.13.1.1 A.13.1.3	0,0%
Control de Puertos y Servicios	Administrar (rastreo/control/corrección) la operación continua de uso de puertos, protocolos, servicios en dispositivos de red para minimizar los espacios de vulnerabilidad disponibles para los atacantes	Control 9	PR-IP	1.4	A.9.1.2 A.13.1.1 A.13.1.2 A.14.1.2	0,0%
Defensa Perimetral	Detectar/prevenir/corregir el flujo de información que se transfiere entre diferentes redes con un enfoque de protección de datos	Control 12	DE-DP	1.1-1.3 8.3 10.8 11.4	A.9.1.2 A.12.4.1 A.12.7.1 A.13.1.1 A.13.1.3 A.13.2.3	0,0%
Protección de Email y Web	Minimizar la superficie de ataque y las oportunidades de los atacantes para manipular el comportamiento humano mediante la interacción con navegadores web y correo electrónico	Control 7	PR-PT			68,6%
Defensa de punto final (Endpoints)	Controlar la instalación, propagación y ejecución de código malicioso en diferentes puntos de la organización, mientras se optimiza la habilidad de defensa, recolección de información y se aplican acciones correctivas	Control 8	PR-PT DE-CM	5.1-5.4	A.8.3.1 A.12.2.1 A.13.2.3	0,0%
Protección de plataformas móviles	Minimizar los riesgos expuestos en caso de que las organizaciones permitan utilizar dispositivos móviles en la organización, o que los colaboradores de la organización utilicen los dispositivos móviles para almacenoar, procesar o transmitir datos de la organización					0,0%
Protección de redes inalámbricas	Los procesos y las herramientas usadas para rastrear/controlar/prevenir/corregir el uso seguro de redes inalámbricas en la red local (LAN) , access points, etc.	Control 15	PR-AC	4.3 11.1	A.10.1.1 A.12.4.1 A.12.7.1	48,0%
Protección de Datos	Los procesos y herramientas usados para prevenir una filtración, mitigando sus efectos y asegurando la privacidad e integridad de información crítica acorde a las directrices formales y procesos aprobados.	Control 13,14	PR-DS PR-AC	1.3-1.4 3.6 4.1-4.3 7.1-7.3 8.7	A.8.3.1 A.9.1.1 A.10.1.1 - A.10.1.2 A.13.2.3 A.18.1.5	0,0%
Endurecimiento de Servidores y Estaciones de trabajo	Capacidades que permitan a las organizaciones implementar buenas prácticas de seguridad de la información en las configuraciones de equipos que serán utilizados en los ambientes de producción.					0,0%
Control de acceso físico	Visualizar los controles necesarios en las organizaciones, que permitan controlar el acceso a las áreas de procesamiento, transmisión y almacenamiento de datos críticos de los usuarios de sus servicios.					80,0%
Monitoreo y Análisis	Recolección, gestión y análisis de logs de eventos que podrían ayudar a detectar, entender o recuperar de un ataque	Control 6	DE-AE RS-AN	10.1-10.7	A.12.4.1 - A.12.4.4 A.12.7.1	0,0%
					A.9.1.1	

Validación de la propuesta

Con el desarrollo de este modelo, se identificó las fortalezas y vulnerabilidades que se presentan en el instituciones y se planteó planes estratégicos para minimizar estas falencias presentes, con la finalidad de proteger los datos importantes que tienen la empresas, de la misma forma se capacitó a los empleados involucrados en este ejercicio para que el uso de esta herramienta sea adecuado y el manejo de los controles sean efectivos a la hora de aplicarlos y así evitar incidentes en la información que podrían generar pérdidas económicas en el sector empresarial.

Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 1

Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Empresas aseguradoras del Ecuador	Seguridad de la información. Modelo de madurez de la información Normativas para medir la seguridad de la **información.**	Enfoque cualitativo	Investigación de campo Investigación bibliográfica	En la presente investigación se identificó las fortalezas y vulnerabilidades de las aseguradoras más grandes del Ecuador, por medio del modelo de madurez de la información que estuvo enfocado en la normativa ISO 27032 y los estándares las normativas internacionales como son la SANS 6.0, NIST CF, PCI 3.0.	Entrevista a los directores de riesgos o similares roles de las 5 empresas del sector asegurador de Ecuador valoradas por los valores de Prima Neta Retenida obtenidos en la Superintendencia de Bancos y Seguros.

CONCLUSIONES

- La norma ISO 27032, en la cual, se enfocó el desarrollo del modelo, permitió acoplar a la empresa para realizar una correcta evaluación de la seguridad de la información y la madurez de los procesos que se realizan en la misma.
- De igual forma con el desarrollo de este modelo distribuido en 5 capas se permitió constatar de forma más exacta el estado actual de los diferentes controles de seguridad de la información en las organizaciones y mostrar las diferentes deficiencias o oportunidades de mejora con las que cuenta la organización, de esta forma se podrá mediante un plan de trabajo mejorar los niveles de madurez obtenidos y así optimizar de la credibilidad y competitividad dentro del ámbito empresarial.
- Con el desarrollo de un modelo para evaluar la madurez de seguridad de la información de las empresas del sector de aseguradoras del Ecuador, se pudo identificar las brechas que tienen las organizaciones como también las fortalezas que poseen, de esta forma, enfocarse en la solución para llegar al nivel de seguridad de la información que las empresas requieren, previniendo vulnerabilidad, robo o manipulación de los datos que tienen las organizaciones.

RECOMENDACIONES

- Se recomienda realizar un análisis exhaustivo para medir el nivel de madurez de la información de las empresas aseguradoras para disminuir los riesgos y vulnerabilidades que tiene la información, para así tener una correcta seguridad de la información.
- Se sugiere realizar pruebas piloto antes de implementar el modelo para medir la seguridad de la información, de esta forma se identificará los problemas reales en la empresa y definir los correctos lineamientos para evaluar estos procesos.
- Por otra parte, para tener resultados positivos y precisos se recomienda realizar evaluaciones constantes y actualización del modelo que permitirá medir el nivel de madurez de la información, de esta forma se valorará el nivel de riesgo de la información en tiempo real, para comparar con análisis anterior y observar las mejoras de seguridad y cuales presentan falencias a solucionar.
- De igual forma, es pertinente tomar en cuenta los resultados obtenidos en los análisis para medir el nivel de madurez de la información y así mejorar las vulnerabilidades que tiene la seguridad de la información aplicando técnicas y estrategias de seguridad informática.
- Finalmente, se recomienda impartir, por medio de expertos en seguridad informática, capacitaciones al personal involucrado en estos procesos, con la finalidad de generar conciencia sobre la importancia de la seguridad de la información en la institución.

BIBLIOGRAFÍA

Advisera, Introducción a los aspectos básicos en normativas de Seguridad - ISO 27001. Versión de implementación: https://advisera.com/27001academy/es/que-es-iso-27001/

Atencio, E. (2019). Diseño de un sistema de gestión de seguridad de la información basado en la NTP-ISO/IEC 27001:2014 para la dirección general de informática y estadística de la Universidad Nacional Daniel Alcides Carrión Pasco Perú. Obtenido de Universidad Nacional Daniel Alcides Carrión: http://repositorio.undac.edu.pe/bitstream/undac/1474/4/T026_10133566_M.pdf

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management. *Business & Information Systems Engineering*, 213-222. doi:https://doi.org/10.1007/S12599-009-0044-5

Bernal Torres, C. A. (2016). *Metodología de la investigación Administración, economía, humanidades y ciencias sociales.* Colombia: PEARSON.

Cano, J., & Almanza, A. (2020). Study of the evolution of Information Security in Colombia. 2000-2018. *Risti. Revista Ib rica de Sistemas e Tecnologias de Informa*, 470-483.

Capelo, M., & Sotomayor, M. (2018). Desarrollo y aplicación de un modelo para evaluar el nivel de madurez de Gestión de Seguridad de la información en Instituciones de Salud Pública en Cuenca. UEES. *Universidad Espíritu Santo*, 1-32.

Cruz, Y., & Martinez, C. (2018). ISO / IEC 27001 aseguramiento de la calidad de la información: Línea de tiempo. *Revista Polo Del Conocimiento, 3(6)*, 478-491. doi:https://doi.org/10.23857/PC.V3I6.641

Figueroa, J., Rodríguez, R., Bone, C., & Saltos, J. (2018). La seguridad informática y la seguridad de la información. *Revista Polo Del Conocimiento, 2(12)*, 145-155. doi:https://doi.org/10.23857/PC.V2I12.420

García, J., Huamani, S., & Lomparte, R. (2018). Modelo de gestión de riesgos de seguridad de la información para PYMES peruanas. *Revista PeRuanade ComPutaCióny sistemas*, 47-56. doi:https://doi.org/10.15381/rpcs.v1i1.148

Gené, J., Gallo, P., & De Lecuona, I. (2018). Big data y seguridad de la información. *Atencion Primaria, 50(1)*, 3-5. doi:https://doi.org/10.1016/J.APRIM.2017.10.004

Hernández-Sampieri, R., & Mendoza Torres, C. P. (2018). *Metodología de la Investigación.* México: McGRAW-HILL.

Holguín, F., & Lema, L. (2019). Modelo para Medir la Madurez del Análisis de Riesgo de los Activos de Información en el contexto de las Empresas Navieras. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, 1-17. doi:https://doi.org/10.17013/risti.31.1-17

Infosegur. (2022). Seguridad informática. Objetivos de la seguridad informática. (https://infosegur.wordpress.com/tag/disponibilidad/).

ISACA. (2019). *COBIT*. Obtenido de ISACA: https://www.isaca.org/resources/cobit

ISOTools Excellence. (2015). *ISO/IEC 17799 Política de seguridad*. Obtenido de ISOTools Excellence: https://www.pmg-ssi.com/2015/04/isoiec-17799-politica-de-seguridad/

Ladino, M., Villa, P., & López, A. (2011). Fundamentos de ISO 27001 y su aplicación en las empresas. *Scientia Et Technica, XVII, 47*, 334-339.

López, D. (2017). Modelo de gestión de los servicios de tecnología de información basado en COBIT, ITIL e ISO/IEC 27000. *Revista Tecnológica - ESPOL, 30(1)*, 51-69.

Mifsud, E. (2012). *MONOGRÁFICO: Introducción a la seguridad informática - Seguridad de la información / Seguridad informática*. Obtenido de Observatorio Tecnologico: http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

Ministerio de Telecomunicaciones y de la Sociedad de la Informacion. (2018). *Guia para la gestión de riesgos de seguris de la informacion.* Obtenido de https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-GESTI%C3%93N-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N-ABRIL-2020.pdf

Niño, N. (2018). *Modelo de un sistema de gestion de seguridad de infromacion - SGSI, para fortalecer la Confidencialidad, Integridad, Disponibilidad y Monitorear los activos de información para el Instituto Nacional de Estadística e Informática INEI-Filial Lambayeque.* Obtenido de Universidad Nacional "Pedro Ruiz Gallo": https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/5935/BC-TES-TMP-788%20NI%c3%91O%20MORANTE.pdf?sequence=1&isAllowed=y

PCI. (2008). *Industria de Tarjetas de Pago (PCI) Normas de seguridad de datos. Requisitos y procedimientos de evaluación de seguridad.* Obtenido de Security Standards Counci: https://listings.pcisecuritystandards.org/pdfs/pci_dss_spanish.pdf

PCI. (2013). *PCI (industria de tarjetas de pago) Normas de seguridad de datos. Requisitos y procedimientos de evaluación de Seguridad. Security Standars Council, 3.* Obtenido de Security Standards Counci: https://fdocuments.ec/document/pci-industria-de-tarjetas-de-pago-normas-de-seguridad-de-datos.html?page=1

Ramirez, J. (2021). *Estrategia a partir de un análisis de vulnerabilidades para evaluar la seguridad de la información en la Alcaldía Barbosa Antioquia.* Obtenido de Universidad Pontificia Bolivariana: https://repository.upb.edu.co/bitstream/handle/20.500.11912/8216/Estrategia%20a%20partir%20de%20un%20an%c3%a1lisis%20de%20vulnerabilidades%20para%20evaluar%20la%20seguridad.pdf?sequence=1&isAllowed=y

Task, J. (2020). *Security and Privacy Controls for Information Systems and Organizations.* doi:https://doi.org/10.6028/NIST.SP.800-53r5

Technopedia. NIST 800-53

https://es.theastrologypage.com/nist-800-53#:~:text=NIST%20800-53%20es%20publicado%20por%20el%20Instituto%20Nacional,informaci%C3%B3n%20y%20promover%20la%20seguridad%20de%20la%20informaci%C3%B3n.

ANEXOS

ANEXO 1

FORMATO DE ENCUESTA

GUIA DE ENCUESTA

Modelo para la evaluación del nivel de madurez de seguridad de la información

1. Tamaño de la empresa.
2. ¿En qué provincia del Ecuador se encuentra ubicada su empresa?
3. ¿Considera importante que la empresa utilice un modelo para medir el nivel de madurez de la seguridad de la información?
4. ¿Utiliza algún modelo para medir el nivel de madurez de la información de su empresa?
5. ¿Qué modelo utiliza para medir el nivel de madurez?
6. ¿Qué modelos para la evaluación de nivel de madurez de la seguridad de la información conoce?
7. ¿Cree usted que un modelo para medir el nivel de madurez de la información ayudará a proteger los datos de su empresa?
8. ¿Estaría dispuesto a utilizar un modelo para medir el nivel de madurez de la información de su empresa?