Diseño de una estrategia del sistema de Seguridad de la Información en la Empresa AyA: Un enfoque desde la gerencia de proyectos

Wilson Alexis Fonseca Pardo

Director

Edward Fernando Toro Perea

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas Tecnología e Ingeniería

Maestría en Gerencia de Proyectos

2024

Resumen

La opción de trabajo de grado es proyecto aplicado donde se realiza un diagnóstico y se presentan los resultados de las problemáticas relacionas con las áreas de estudio.

El trabajo está basado en la dirección de proyectos bajo los lineamientos de la gerencia de proyectos haciendo énfasis en Sistemas de Gestión de Seguridad de la Información (SGSI), donde se logra el éxito del proyecto al seleccionar la mejor estrategia que garantice la protección de la información.

La estrategia establecida permite a los colaboradores de AyA participar en cada etapa del proyecto desde las áreas de Mesa de Ayuda, Implementación, Mercadeo, Recurso Humanos y Tecnología.

En AyA se ha detectado la falencia determinando que es necesario contar con una estrategia de gestión basado para ejecutar los proyectos aplicando buenas prácticas, para mejorar el manejo de recursos aumentando la inversión controlando el tiempo de ejecución y la calidad del Sistema de Gestión de Seguridad de la Información.

Es necesario implementar un Sistema de Seguridad de la Información en la empresa AyA con la finalidad de garantizar la integridad, confidencialidad y disponibilidad de la información para mejorar procesos internos y garantizar al cliente externo que su información estará segura bajo la estrategia seleccionada.

Palabras Clave: Gerencia de proyectos, Gestión de seguridad de la información, Riesgos en la seguridad de la información, Estándares de seguridad de la información, Estrategia de un sistema de gestión.

Abstract

The degree work option is an applied project where a diagnosis is made and the results of the problems related to the study areas are presented.

The work is based on project management under the project management guidelines emphasizing Information Security Management Systems (ISMS), where the success of the project is achieved by selecting the best strategy that guarantees the protection of the information. information.

The established strategy allows AyA collaborators to participate in each stage of the project from the Help Desk, Implementation, Marketing, Human Resources and Technology areas.

In AyA, the shortcoming has been detected, determining that it is necessary to have a management strategy based on executing the projects applying good practices, to improve resource management by increasing the investment, controlling the execution time and the quality of the Safety Management System. information.

It is necessary to implement an Information Security System in the AyA company in order to guarantee the integrity, confidentiality and availability of information to improve internal processes and guarantee the external client that their information will be safe under the selected strategy.

Keywords: Project management, Information security management, Information security risks, Information security standards, Management system strategy.

Tabla de contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

Para desarrollar una estrategia del sistema de gestión de seguridad de la información se realizará un diagnóstico para conocer la manera cómo el departamento de tecnología y colaboradores garantiza actualmente la seguridad de la información utilizando herramientas de gestión de proyectos como árbol de problemas, mapas de empatía, entrevistas y encuestas para realizar el análisis de la problemática actual y así determinar las posibles alternativas de estrategias de gestión de seguridad de la información y seleccionar la estrategia más acorde a las necesidades y requerimientos técnicos de la empresa AyA.

Es necesario una estrategia del sistema de seguridad de la información en la empresa AyA con la finalidad de garantizar la integridad, confidencialidad y disponibilidad de la información para mejorar procesos internos y garantizar al cliente externo que su información estará segura bajo los estándares de la seguridad de la información.

En estos momentos en la AyA para acceso a las aplicaciones se cuenta con usuarios genéricos para ingresar a las aplicaciones sin perfilamiento alguno, donde en caso de presentarse cambios o pérdida de información se desconocería la persona generadora del evento.

Para encontrar la estrategia más acorde de acuerdo a las necesidades de la empresa AyA es importante la gestión de proyectos la cual permite definir claramente el alcance de la estrategia y los objetivos a lograr proporcionando un marco estructurado para la planificación detallada de la estrategia identificando tareas, asignación de recursos asegurando que las actividades se realicen de manera organizada y eficiente facilitando el seguimiento y control continuo del progreso de la estrategia proporcionando herramientas para monitorear el rendimiento, identificar desviaciones y realizar ajustes según sea necesario para mantenerse en

camino con los objetivos. La implementación de una estrategia implica cambios en la organización donde la gestión de proyectos aborda la gestión del cambio al planificar y comunicar efectivamente los cambios. Las estrategias involucran varias iniciativas interrelacionadas donde la gestión de proyectos facilita su integración garantizando una alineación coherente con los objetivos evitando la duplicación de esfuerzos.

La gestión de proyectos es un componente esencial en la ejecución exitosa de una estrategia al proporcionar la estructura y las herramientas necesarias para asegurar que se logren los objetivos de manera eficiente y efectiva.

El proceso del diseño de la estrategia del SGSI iniciará desde la etapa de levantamiento de información para conocer las debilidades de la empresa para diseñar y planear la forma de establecer las normas y políticas causando el menor impacto en el personal por medio de la concientización.

Al terminar la estrategia del SGSI prosigue la etapa de hacer perdurar dichas normas y políticas en el tiempo, actividad a desarrollar por medio de controles, seguimientos y auditorías.

Hoy es importante contar con un sistema de gestión de seguridad de la información donde se evidencia al mirar las estadísticas globales donde se percibe un aumento del 45% en certificados de SGSI. El número de certificados ISO va creciendo cada año en Sudamérica, sin embargo todavía no se sitúa algún país en el top 10 de los países con mayor número de certificados. Colombia cuenta con 163 certificaciones por año, cifra muy baja partiendo de la necesidad de evitar riesgos de pérdidas financieras, reducción de la productividad, reputación de la empresa y multa por no garantizar la protección de datos estipulada en la legislación vigente establecida desde el año 2002 reglamentada en la ley 1581. Este último riesgo impacta a la empresa AyA al manejar las historias clínicas de todas las EPS de Cafam y Nueva EPS.

Yhonathan Gómez, especialista jurídico de Latam señala que, “de acuerdo con la experiencia, la sustracción de cantidades económicas por datos financieros y la suplantación de identidad son los principales riesgos que enfrentan los datos de las personas en entorno digitales. Ante ese escenario, este tipo de normativas pretenden responder justamente a esos desafíos de seguridad, brindando a la población un marco legal y jurídico que proteja su integridad y la de su información personal” (Tivit Latam, 2021).

Implementar una estrategia del sistema de seguridad de la información es de vital importancia para certificarse en la ISO27001, porque ello brinda seguridad y confianza a las empresas a las cuales se les prestan los servicios de software a nivel de implementación y accesos y a su vez dichas empresas cuentan con sistemas de seguridad de la información y desean implementar políticas conjuntas para evitar fuga o manipulación de datos.

Es importante contar con SGSI porque abre las puertas a los inversionistas nacionales y extranjeros, préstamos bancarios con miras ampliar mercados en las bolsas de valores.

Pero no sólo es implementar el SGSI sobre los aplicativos actuales, se deben crear políticas de seguridad desde el código software para evitar cambios en los desarrollos generando reprocesos y crear productos y servicios con estándares internacionales que sean adquiridos en cualquier parte del mundo, garantizando su permanencia en el tiempo.

Planteamiento del problema

Es necesario planear un sistema de gestión de seguridad de la información para garantizar la seguridad de los activos de la empresa que son software e información la cual debe garantizar la disponibilidad, integridad y confiabilidad con la finalidad de mostrar una mayor imagen de confianza del cliente interno y externo, dando el valor agregado de credibilidad por lo cual se aplicarán técnicas y herramientas como el árbol de problemas y mapa de empatía para seleccionar la mejor estrategia.

Si la empresa AyA contara con una estrategia del sistema de gestión de seguridad de la información puede agilizar y gestionar procesos de manera segura ,y de esta manera preparar al personal para certificarse, lo cual es una ventana para mantener clientes satisfechos al ver que su información está protegida y a su vez es una entrada a nuevos clientes quienes al momento de compartir el activo más importante de cualquier empresa la información lo hacen en medio de la desconfianza y la precaución, y la certificación en seguridad de la información es la puerta de transacciones seguras donde cada bit será protegido.

Lo anterior se sustenta en los datos suministrados por la Fiscalía General de la Nación donde en el presente año 2021 se han reportado 30.000 ataques cibernéticos, en comparación al años 2020 con un reporte del 8.290 casos de ataques cibernéticos, los cuales se generan por no implementar o mala implementación de un Sistema de Gestión de Seguridad de la información. Bogotá con 8.355 casos, Medellín 1.664 y Cali con 1.569. son las ciudades con mayor afectación (Barbosa y Mancera, 2022). Es por ello que el Tanque de Análisis y Creatividad de las TIC (TicTac) invitan a las empresas a buscar recursos tecnológicos para proteger la información que es considerado el activo más valioso. Para Juan Hover González, gerente Seguridad Información de Claro Colombia, “el foco en post-pandemia es proporcionar mejores formas para identificar y

abordar de forma proactiva las vulnerabilidades potenciales antes de que éstas puedan ser aprovechadas por los atacantes. Por eso es necesario implementar plataformas de multiple- factor de autentificación, revisar los flujos de sus aplicaciones, consulte con fabricantes de tecnología de seguridad sobre la detección y respuesta de amenazas de endpoints (EDR) y complemente con un Antimalware con funciones avanzadas. Así mismo, contar con un servicio de correo seguro y afinar su Firewall de Aplicaciones (WAF) que responda inmediatamente a paquetes malformados o firmas de ataques identificables y, por último, realice pruebas de seguridad permanente" (SAFE, 2021).

De esta manera plasmar una estrategia del SGSI en la empresa AyA es importante hacerlo de manera guiada por medio de un sistema de gestión de proyectos donde se garantice el cumplimiento de objetivos, plazos y presupuesto manteniendo la visión de éxito impactando positivamente los nuevos cambios en la organización al dar los parámetros para la protección de datos sensibles cumpliendo con la normatividad legal aprendiendo a gestionar los riesgos para garantizar la continuidad del negocio mejorando la eficiencia de procesos demostrando un serio compromiso con la seguridad de la información.

Pero no siempre la estrategia de un SGSI puede ser exitosa, al tener una insuficiente planificación y gestión de proyectos tal como no realizar seguimientos periódicos, escasa comunicación, falta de trabajo en equipo, deficiente asignación de recurso humano y roles, ausencia de una correcta metodología, pueden generar retrasos o no viabilidad del proyecto. Por ello es importante no solo hacer seguimiento al momento de ejecución, el seguimiento se debe realizar desde el momento de la planeación para garantizar la calidad del producto o servicio a entregar cumpliendo con todas las etapas, actividades y tareas establecidas bajo las herramientas de gerencia de proyectos.

¿Cómo por medio del uso de las herramientas de gestión de proyectos puedo sustentar el desarrollo de una estrategia del sistema de gestión de seguridad de la información de la empresa AyA?

Objetivos

Objetivo General

Desarrollar una estrategia del sistema de gestión de seguridad de la información basado en los lineamientos de la gerencia de proyectos.

Objetivos específicos

Realizar un diagnóstico para la determinación de una estrategia de un sistema de gestión de seguridad de la información en la empresa AyA.

Analizar una estrategia de un sistema de gestión de seguridad de la información en la empresa AyA.

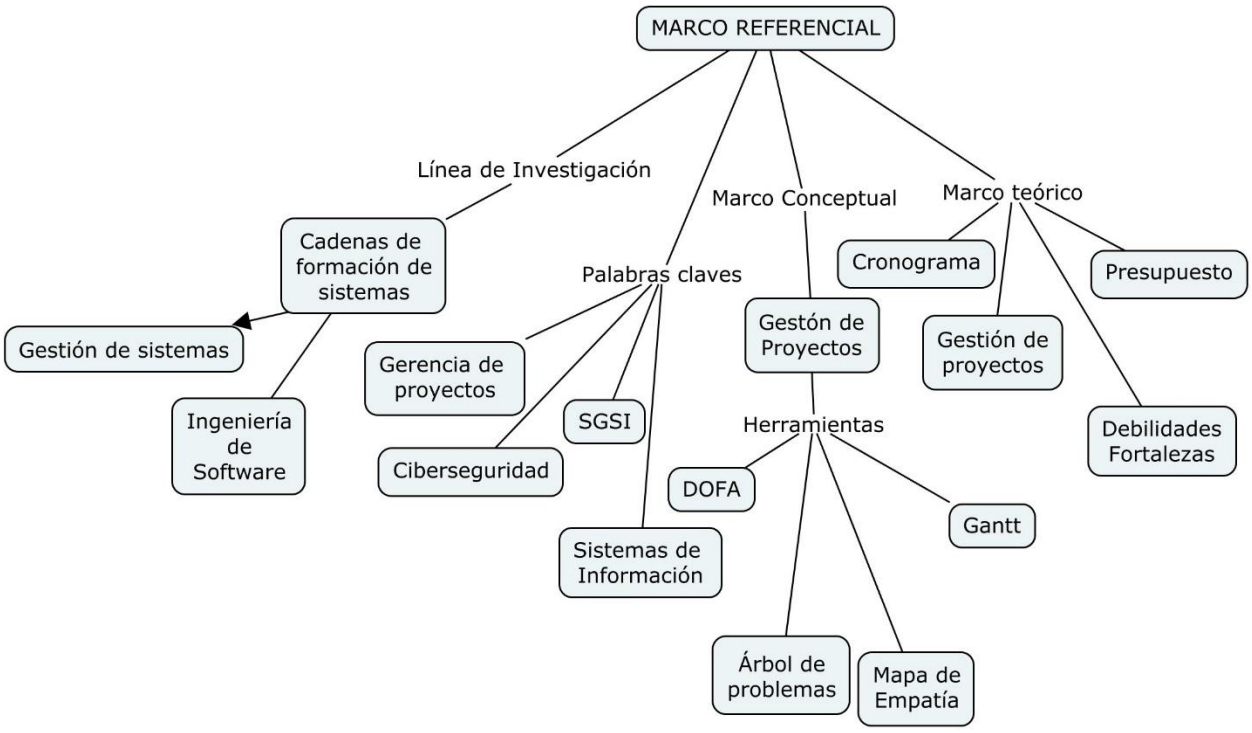
Evaluar una estrategia del sistema de gestión de seguridad de la información en la empresa AyA.

Mapa Conceptual

Se diseña el mapa conceptual presentando el marco referencial para conocer los conceptos claves desglosando la información en unidades más simples para conocer el orden lógico y jerárquico donde se conocerá la línea de investigación a la cual pertenece el proyecto, igualmente las palabras claves la cuales indican los ítems base del proyecto y las herramientas a utilizar para alcanzar los objetivos de estudio.

Figura 1

Mapa conceptual



Nota. La figura muestra el contenido más relevante para la realización del proyecto de investigación.

Marco de referencia

En el marco de referencia se presentan los criterios y parámetros estableciendo los límites del proyecto identificando los recursos y herramientas disponibles para conocer su alcance y límites.

Las herramientas las cuáles nos van a permitir crear una estrategia de un sistema de seguridad de la Información en la empresa AyA son las relacionadas con la gestión de proyectos.

Las herramientas de gestión de proyectos son fundamentales para determinar una estrategia efectiva de un Sistema de Gestión de Seguridad de la Información organizando la complejidad del proyecto y a mantener un enfoque ordenado.

Las herramientas permiten examinar el diagnóstico del sistema de seguridad de la información de la compañía AyA; mediante el uso de herramientas; con el propósito de buscar múltiples alternativas de la estrategia del sistema de gestión de seguridad de la información.

Además de evaluar las posibles alternativas del sistema de gestión de seguridad de la información de la compañía AyA; mediante el uso de herramientas de valoración; para la determinación de la estrategia del sistema de seguridad de la información de la compañía AyA.

De esta manera determinar las características del sistema de gestión de seguridad de la información de la compañía AyA; por medio de datos, entrevistas, encuestas y Matriz DOFA; con el fin de determinar el diagnóstico de la estrategia de gestión de mejoramiento del sistema de seguridad.

Marco conceptual

Las herramientas de la gestión de proyectos a utilizar para la recolección y transformación de datos para crear la estrategia del sistema de gestión de seguridad de la información:

DOFA

El análisis DOFA, también conocido como análisis SWOT en inglés (Strengths, Weaknesses, Opportunities, Threats), es una herramienta utilizada en la gestión de proyectos (Kotler, Armstrong. 2018). Es una herramienta de estudio de las situaciones del proyecto analizando sus características internas y externas, donde nos permite validar las Debilidades, Oportunidades, Fortalezas y Amenazas, y de esta forma tener un diagnóstico real del proyecto.

Así se conocerán los puntos débiles identificando los posibles problemas conociendo los procesos a mejorar en la organización o proyecto.

Diagrama de Gantt

El diagrama de Gantt se utiliza como una herramienta gráfica en la gestión de proyectos para representar visualmente la planificación y programación de tareas a lo largo del tiempo Martín, C, 2021).

De esta manera se pueden gestionar proyectos, determinar la logística de las tareas y supervisar el progreso del proyecto.

Mapa de empatía

El mapa de empatía es una representación gráfica que ayuda a comprender de manera profunda a los usuarios de un producto o servicio. Se divide en secciones que incluyen aspectos como lo que piensa y siente el usuario, lo que ve y escucha, sus necesidades y objetivos, así como los desafíos que enfrenta. Este enfoque ayuda a los equipos de diseño y desarrollo a

ponerse en los zapatos de los usuarios para tomar decisiones más informadas (Gray & Macanufo, 2018).

Con la herramienta se busca describir las necesidades del cliente por medio de 6 aspectos relacionados con el ser humano y de esta manera comprender los productos o servicios que se desean ofrecer.

Árbol de problemas

El árbol de problemas es una herramienta utilizada para analizar y visualizar las causas fundamentales de un problema específico identificando posibles obstáculos y problemas durante la ejecución de proyecto (Kerzner, H. 2017).

Open Project

Es una herramienta de gestión de proyectos de código abierto que se utiliza para planificar, colaborar y gestionar proyectos de manera efectiva. Ofrece características como seguimiento de tareas, gestión de documentos, seguimiento del tiempo y colaboración en equipo (OpenProject Community, 2020).

Marco teórico

El marco teórico se describen las herramientas de gestión de proyectos las cuales se utilizarán para el desarrollo de las actividades del proyecto con a la finalidad de conocer la problemática actual y evaluar las mejores alternativas para la consecución de la estrategia del sistema de gestión de seguridad de la información.

DOFA

Por medio de DOFA se realizará el análisis de Debilidades, Oportunidades, Fortalezas y Amenazas presentes que pueden beneficiar o afectar el proyecto de implementación de un Sistema de Gestión se Seguridad de la Información en AyA Software.

Figura 2

Dofa

Nota. La figura muestra las partes que constituyen la matriz Dofa para conocer la situación rela de una organización.

Diagrama de Gantt

Con el diagrama de Gantt se visualizan las fechas de inicio y finalización de las tareas asignadas y responsables, donde las tareas están organizadas en orden cronológico y relacionadas donde una actividad es el complemento de la anteriormente ejecutada. Además cada tarea hace parte del cronograma y se le asigna un presupuesto, de esta forma Gantt indicará si el proyecto está dentro de los plazos establecidos o va a presentar problemas financieros.

Figura 3

Diagrama de Gantt

PLAN DEL PROYECTO Y PLANTILLA DEL GRÁFICO DE GANTT

NOMBRE DEL PROYECTO	ADMINISTRADOR DEL PROYECTO	FECHA DE INICIO	FECHA DE FINALIZACIÓN	PROGRESO GENERAL
Lanzamiento del producto	Alex B.	2-Sep	10-Oct	20%

RESULTADO DEL PROYECTO

DECLARACIÓN SOBRE EL ALCANCE

TAREAS	RESPONSABLE	INICIO	FINALIZACIÓN	DÍAS	ESTADO
Definir la reunión de lanzamiento	Alex B.	2-Sep	3-Sep	2	Completo
Acordar los objetivos	Frank C.	3-Sep	7-Sep	5	Completo
Requisitos detallados	Jacob S.	7-Sep	12-Sep	6	Completo
Requisitos de hardware	Jacob S.	9-Sep	11-Sep	3	Atrasado
Plan definitivo de recursos	Jacob S.	11-Sep	15-Sep	5	En curso
Dotación de personal	Alex B.	16-Sep	17-Sep	2	En curso
Requisitos técnicos	Frank C.	17-Sep	21-Sep	5	No se ha iniciado
Desarrollo de la base de datos	Shari W.	22-Sep	24-Sep	3	No se ha iniciado
Desarrollo de API	Shari W.	23-Sep	27-Sep	5	No se ha iniciado
Cliente de la interfaz de usuario	Alex B.	25-Sep	29-Sep	5	No se ha iniciado
Pruebas	Kennedy K.	24-Sep	2-Oct	9	No se ha iniciado
Desarrollo completo	Jacob S.	2-Oct	5-Oct	4	No se ha iniciado
Configuración de hardware	Alex B.	5-Oct	7-Oct	3	No se ha iniciado
Pruebas del sistema	Kennedy K.	6-Oct	9-Oct	4	No se ha iniciado
Presentación		9-Oct	10-Oct	2	

Nota. La figura muestra las partes que constituyen un diagrama de Gannt para hacer seguimiento a los proyectos.

Mapa de empatía

Como ante sala a la estrategia del SGSI se socializará el proyecto tomando como base los resultados del mapa de empatía para comprender las necesidades del cliente al ser participe en cada etapa al entender las expectativas conociendo lo que piensa, oye, ve, esfuerzos y resultados.

Figura 4

Mapa de empatía

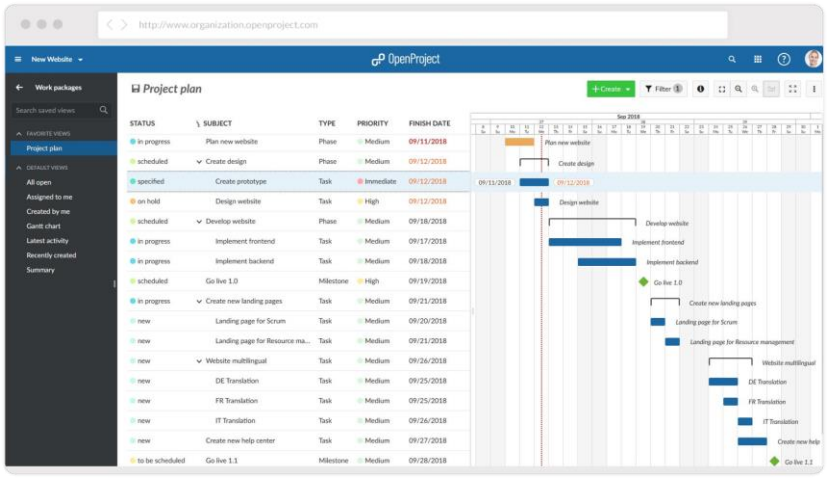
Nota. La figura muestra las seis divisiones que conforman el mapa de empatía. Adaptado de designthinking, (https://designthinking.gal/el-mapa-de-empatia/)

Open Project

Para la gestión de presupuesto se utilizará el software Open Project para llevar el control presupuestal dividiendo el valor total en su mínima parte para ello estableciendo un costo a cada actividad a desarrollar con su respectiva fecha de inicio y fin.

Figura 5

Open Project



Nota. La figura muestra la interfaz gráfica de la herramienta Open Project.

Herramienta Costo/ Beneficio

Una herramienta costo/beneficio es un enfoque o método utilizado para evaluar y comparar los costos relativos y los beneficios asociados con la implementación de un proyecto, programa o decisión. El objetivo principal es determinar si los beneficios obtenidos justifican los costos incurridos y si la inversión es económicamente viable. Esta herramienta es comúnmente utilizada en la toma de decisiones empresariales y gubernamentales para evaluar la rentabilidad y la eficiencia de diversas opciones.

Marco histórico

La evolución de la gerencia de proyectos ha sido un proceso dinámico que ha respondido a los cambios en la tecnología, la economía y las expectativas de los stakeholders. A continuación, se presenta una descripción general de la evolución de la gerencia de proyectos:

A principios del siglo XX, Taylor y Gantt introdujeron principios de gestión científica y gráficos de Gantt dando las bases para la gestión eficiente del tiempo y los recursos en los proyectos donde el enfoque en las relaciones humanas en el trabajo influyó en la gestión de proyectos al reconocer la importancia de la motivación y el liderazgo.

La gestión de proyectos se vio influenciada por la idea de que no existe un enfoque único donde se deben adaptar a las circunstancias del entorno.

Ya en la década del 50 inicia el desarrollo de técnicas como el Método de la Ruta Crítica (CPM) y la Técnica de Revisión y Evaluación de Programas (PERT) para gestionar proyectos grandes y complejos.

A finales del siglo XX se desarrolla el enfoque ágil destacando la flexibilidad, colaboración y la entrega incremental en la gestión de proyectos.

Sobre la década del 70 el Proyecto Management Institute (PMI) establece las herramientas del PMI publicando eel primer "Body of Knowledge" (PMBOK) en 1983.

Enfoque en Proyectos de Construcción: La gerencia de proyectos se centró principalmente en la construcción y sectores de ingeniería.

En la década del 90 con el auge de la Tecnología de la Información y crecimiento de la industria de TI se adoptaron enfoques más ágiles y orientados a resultados publicándose El Manifiesto Ágil en 2001, dando origen a las metodologías ágiles como Scrum y Kanban.

Década de 2000 globalización y complejidad, aumento de la complejidad y la globalización de los proyectos, lo que llevó a una mayor atención en la gestión de riesgos y la adaptabilidad.

Enfoque en la Gestión del Valor: Mayor énfasis en entregar valor al cliente y enfoques más centrados en el cliente.

En la década del 2010 empieza la transformación Digital con la Integración de tecnologías emergentes, como la inteligencia artificial y la analítica de datos, en la gestión de proyectos.

Más allá de la ingeniería se da la expansión de la gerencia de proyectos a sectores como el desarrollo de software, marketing y servicios.

Desde la década actual 2020 surge un enfoque en sostenibilidad para la gestión de proyectos socialmente responsables donde la pandemia COVID-19 aceleró la adopción de enfoques remotos y la colaboración en línea en la gestión de proyectos.

La tendencia actual es la adopción de enfoques híbridos combinando prácticas ágiles y tradicionales dando importancia a las habilidades blandas como la comunicación efectiva y el liderazgo (Morelos, 2023).

La evolución de la gerencia de proyectos refleja la necesidad de adaptarse a las cambiantes condiciones del entorno empresarial y tecnológico. La diversificación de enfoques y la incorporación de tecnologías emergentes continúan dando forma a la disciplina de la gestión de proyectos.

Estado del arte

En el proyecto de un sistema de gestión de seguridad de la información (SGSI) aplicado a la organización ABC indican que en toda organización existen desafíos relacionados con la

seguridad de la información para proteger cada uno de los activos de información. Los planes de acción y buenas prácticas permiten mitigar las vulnerabilidades que corromper la información de la organización. Establecer un programa de seguridad de la información debe ser considerado como primer paso para las áreas de IT para mantener una completa integridad, disponibilidad, confidencialidad y privacidad en los datos de la organización (Safla, E. 2021).

En la propuesta de un sistema de gestión de seguridad de la información (SGSI) aplicado a la Institución Financiera COOPELQUINCHELE expresan que la pandemia provocada por el COVID 19, ha conllevado que la información sea uno de los recursos más importantes en las organizaciones. Razón por la cual todas las organizaciones y mucho más las instituciones del sector financiero sin importar el segmento en el cual estén ubicados deberían realizar una apropiada gestión de riesgos (Aules, F.2021).

A nivel de resultados relevantes para la estrategia de un Sistema de Gestión de Seguridad de la Información, según el proyecto aplicado a la empresa SOLTESI S.A.C obtuvo que las incidencias que se efectuaban en la empresa y no se solucionaban al 99% implementando el SGSI con la norma ISO 27001 mejorara significativamente en resolver las incidencias al menor tiempo posible donde se obtuvo un valor media de 32% de incidencias resueltas al mes y que al realizar el post-test se obtuvo un valor media de 75% de incidencias resultas en un mes, siguiendo con el resultado de la confidencialidad on un valor media de 80% de incidencias resultas en un mes y referente a la disponibilidad se obtuvo una media de 81% de incidencias resultas en un mes (Ramos, 2021).

Marco Legal

En el marco legal se presentan las obligaciones, derechos y leyes que se deben tener en cuenta al momento de optar por una estrategia de gestión de seguridad de la información en referencia a la protección de datos.

El marco legal a utilizar la metodología de la estrategia del Sistema de Gestión de Seguridad de la Información (SGSI) en AyA, estará regida por la ley colombiana 1581 de 2012 y el Decreto 1377 de 2013.

Marco normativo

Constitución Política de Colombia Artículo 15, ley 1266 de 2008, ley 1581 de 2012, decreto 1377 de 2013 (Gutierrez & Villegas, 2022).

Metodología

En la metodología del proyecto se presenta el tipo de investigación y procedimientos adecuados para alcanzar los objetivos siendo guía en cada etapa del proyecto para garantizar la eficacia en la consecución de resultados.

Enfoque metodológico

El tipo de investigación a utilizar es cualitativa y exploratoria al destacar los aspectos fundamentales de la problemática encontrando los procedimientos para desarrollar una estrategia del sistema de gestión de seguridad de la información en la empresa AyA bajo los lineamientos de la gerencia de proyectos donde se busca encontrar soluciones a la problemática para mejorar la ejecución del proyecto por medio de los instrumentos técnicos para la recolección de datos como las entrevistas, observación, focus group y fuentes abiertas de información, analizando la información en Excel que es una herramienta del paquete office y el software libre Open Project.

En la estrategia de gestión de seguridad de la información frente a las historias clínicas por la IPS Salud Max S.A.S. (Riascos & Torres, 2022), al aplicar un enfoque cualitativo permite establecer el análisis, la valoración, el tratamiento de riesgos y la implementación de controles de seguridad de la información.

Al no contar con un sistema de la información genera un impacto negativo del daño afectando directamente los procesos de la información y generando posibles sanciones a la organización por no contar con un proceso de protección de la información acordes con la normatividad vigente (Riascos & Torres, 2022).

Según Gustavo Betarte es un hecho que los sistemas de gestión y de información están muy arraigados en los procesos productivos, industriales, de servicios, gubernamentales y casi cualquier sector activo de la sociedad. La de los sistemas de información requiere dotar de

seguridad para preservar la calidad de los servicios y dar valor a los activos. Ya no es suficiente actuar de modo reactivo y defensivo, se requiere de un sistema de gestión de seguridad de la información (SGSI) proactivo. Existen diferentes estándares que se desarrollaron para gestionar la seguridad de la información, algunos centrados en la gestión de riesgos (ISO27001), y otros incluso tendientes a desarrollar un modelo de madurez de la seguridad de la información (ISM3).

Se deben analizar diferentes enfoques con el fin de proponer una metodología de implementación, gestión y mejora de un SGSI. Se requiere analizar diferentes métodos conocidos de análisis y gestión de riesgos en pro de una metodología eficaz y sostenible, primando un criterio de conveniencia costo-beneficio (Pallas, 2019).

Procedimiento

En el procedimiento se describen las fases relacionadas con los objetivos de la estrategia del sistema de seguridad de la información en la empresa AyA.

Primera Fase Diagnóstico

Etapa I Consecución de información

Actividad 1: Diseñar las preguntas de las entrevistas por medio del mapa de empatía para analizar la problemática actual en la empresa AyA.

Actividad 2: Aplicar las entrevistas para conocer la problemática referente a la ausencia del Sistema de Gestión de Seguridad de la Información.

Actividad 3: Realizar el análisis del problema por medio del árbol de problemas para conocer causas y efectos.

Etapa II Creación del instrumento para determinar la muestra y aplicación de la muestra

Actividad 4: Desarrollar la encuesta por medio de la herramienta del mapa de empatía de acuerdo a los resultados obtenidos en las entrevistas y su respectivo diagnóstico en el árbol de problemas.

Actividad 5: Determinar el tamaño de la muestra a quienes se realizarán las entrevistas.

Actividad 6: Aplicar las encuestas por medio de la herramienta de Google Forms.

Actividad 7: Síntesis de la encuesta realizada a los colaboradores.

Etapa III Análisis de la encuesta utilizando el mapa de empatía y DOFA

Actividad 8: Tabular el resultado de las entrevistas por medio de las herramientas Excel y Google Forms.

Actividad 9: Por medio del mapa de empatía tabular los resultados para conocer las necesidades generadas de la problemática de estudio en AyA.

Actividad 10: Analizar las variables de carácter utilizando la matriz de identificación de problemas para validar las causas y efectos posteriormente con el árbol de problemas.

Actividad 11: Síntesis del diagnóstico integral.

Segunda Fase Tratamiento

Etapa IV Determinar las posibles soluciones de la estrategia de un Sistema de Gestión de Seguridad de la Información (SGSI).

Actividad 12: Analizar el diagnóstico integral mediante la matriz DOFA extendida para conocer las alternativas de solución para desarrollar una estrategia del sistema de gestión de seguridad de la información bajo los lineamientos de la gerencia de proyectos en la empresa AyA.

Actividad 13. Síntesis de las alternativas de solución para el Sistema de Gestión de Seguridad de la Información.

Actividad 14: Determinar los criterios técnicos de las posibles estrategias del Sistema de Gestión de Seguridad de la Información por medio de un cuadro comparativo.

Actividad 15: Analizar las ventajas y desventajas de los criterios técnicos de los Sistema de Gestión de Seguridad de la Información.

Actividad 16: Calificar las alternativas del Sistema de seguridad de la información por utilizado la matriz de ponderación técnica.

Actividad 17: Seleccionar de acuerdo a los resultados obtenidos y en relación a los requerimientos y necesidades de la gerencia el pre- diseño de la estrategia del Sistema de Gestión de Seguridad de la Información (SGSI).

Actividad 18: Síntesis de la fase de las alternativas de seguridad de la información.

Tercera Fase Evaluación

Etapa V Determinar las alternativas para determinar el SGSI

Actividad 19: Consolidar la información y evaluar las alternativas para la elaboración del SGSI y las políticas de Seguridad de la Información.

Actividad 20. Utilizar la herramienta C/B para establecer la mejor estrategia del Sistema de Gestión de Seguridad de la Información.

Actividad 21: Seleccionar la mejor estrategia del Sistema de Gestión de Seguridad de la Información.

Actividad 22: Definir los activos a proteger en el Sistema de Gestión de Seguridad de La Información.

Actividad 23: Determinar la documentación necesaria para establecer la mejor estrategia del Sistema de Gestión de Seguridad de la Información.

Actividad 24: Establecer las políticas de Seguridad de la Información según la mejor estrategia del Sistema de Gestión de Seguridad de la Información.

Etapa VI Finalización del documento

Actividad 25: Conclusiones.

Actividad 26: Recomendaciones.

Diagnóstico del Análisis de resultados de la problemática de la ausencia de una estrategia del Sistema de Gestión de Seguridad de la Información

En el diagnóstico la consecución de la información se realiza por medio de entrevistas al gerente y líderes de áreas para determinar el análisis de la problemática de estudio. Posteriormente se crea el instrumento de la encuesta, seleccionando por medio del mapa de empatía las mejores preguntas para su aplicación y por medio de la herramienta DOFA realizar el análisis del diagnóstico.

Consecución de la información

La información surge ante el riesgo de presentarse fuga y retención de la información por parte d terceros de manera interna o externa.

Al validar las políticas establecidas para garantizar la seguridad de la información se indica que no se ha establecido. Donde sólo empieza a cobrar importancia ante la necesidad del cliente externo por medio de PQR de conocer cómo se protege el activo más valioso que es la información a partir de aplicativos, bases de datos y accesos locativos.

Análisis de la problemática

Para identificar causas y efectos se realizan entrevistas al director de tecnología y líderes de área (Apéndice A) con la finalidad de conocer el estado actual de la compañía para conocer los problemas generados ante la ausencia de un Sistema de Gestión de Seguridad de la Información, realizando las siguientes preguntas por medio de la herramienta Mapa de Empatía.

Diseño de las preguntas de las entrevistas por medio del mapa de empatía para analizar la problemática actual en la empresa AyA.

Para el diseño de las preguntas se utiliza el mapa de empatía en la figura 6 para comprender de manera más profunda necesidades, deseos, comportamientos y motivaciones de los entrevistados.

¿Qué Piensa y Siente?

¿Qué tipos de políticas de seguridad de la información se pueden seleccionar para solventar la problemática actual? ¿La empresa puede brindar soluciones mediante un Sistema de Gestión de Seguridad de la Información?

¿Qué Oye?

¿Queja de los clientes referente al riesgo de vulnerabilidad de la información al no contar con un Sistema de Gestión de Seguridad de la Información?

¿Qué Ve?

¿Se han presentado incidentes de seguridad de la información?

¿Qué Dice y Hace?

¿Tiene planeado realizar cambios en las políticas actuales para proteger la información de la empresa y clientes?

Esfuerzos

¿Cuál es el mayor problema presentado por no contar con un Sistema de Gestión de Seguridad de la Información?

Resultados

¿Cómo le gustaría que funcionara el Sistema de Gestión de Seguridad de la Información?

Figura 6

Mapa de empatía diseño de pregunta

Nota. La figura presenta las preguntas abiertas a realizar a los entrevistados por medio del mapa de empatía.

Perfil de los entrevistados

Las entrevistas se realizarán a los perfiles de la empresa que son determinantes para optar por un Sistema de Gestión de Seguridad de la Información.

El director de Tecnología es la persona quien dirige todos los procesos de tecnología en la organización coordinando las áreas de soporte técnico, infraestructura, Aseguramiento de Calidad de Software e Implementación. (Apéndice A).

La jefe de Implementación es la encargada de capacitar a los clientes externos en los aplicativos de la organización y quien recibe de manera directa las opiniones, sugerencias y/o hallazgos del cliente donde se pueden encontrar incidentes de seguridad. (Apéndice B).

El jefe de Infraestructura también será entrevistado al tener a su cargo el software y hardware de la organización en especial servidores y accesos físicos al edificio donde es la primera área quien descubre y/o escalan incidentes de seguridad. (Apéndice C).

Tabla 1

Resumen entrevistas

ENTREVISTA SEMIESTRUCTURADA			
Preguntas	**Director de Tecnología**	**Jefe de Implementación**	**Jefe de Infraestructura**
¿Qué tipos de políticas de seguridad de la información se pueden seleccionar para solventar la problemática actual?	Sería importante diseñar un Sistema de Gestión de Seguridad de la Información para proteger la información de AyA. Las políticas debe implicar al personal, software, hardware, acceso lógicos y físicos, y almacenamiento.	Como jefe de implementación las políticas que se requieren implementar son la relacionadas con los aplicativos en los ambientes de desarrollo, producción y contingencia.	Desde el área de infraestructura se deben seleccionar políticas para servidores y acceso físico.
¿La empresa puede brindar soluciones mediante un Sistema de Gestión de Seguridad de la Información?	Si, la empresa puede garantizar soluciones con un SGSI para proteger todos los activos de la compañía. No sólo proteger los aplicativos de la	Si, la empresa debe brindar las soluciones de carácter urgente para tener un Sistema de Gestión Informática para facilitar los	Si, la empresa debe brindar las soluciones de seguridad de la información interna y externamente para reducir los riesgos a fallos de la

	compañía. Se debe proteger el acceso al edificio, oficinas y demás.	procesos de capacitación.	infraestructura por un update o upgrade minimizando la posibilidad de ataques.
¿Se han presentado quejas de los clientes referente al riesgo de vulnerabilidad de la información al no contar con un Sistema de Gestión de Seguridad de la Información?	Si, los clientes han solicitado cuáles políticas de seguridad se están utilizando para evitar ataques informáticos al compartir parte de la infraestructura.	Si, al momento de capacitar a los clientes en los aplicativos(software) indican porque no se perciben políticas de seguridad tan básicas como límite mínimo de caracteres y acceso con usuarios genéricos. De parte mía se explica al cliente que en el ambiente de desarrollo no se tienen aplicadas ciertas políticas a diferencia de los ambientes productivos.	Si, al momento de presentarse alguna novedad en las transacciones los clientes indican que no se visualizan restricciones sobre las carpetas y cualquier usuario puede mover, copiar o eliminar la información.
¿Se han presentado incidentes de seguridad de la información?	Si se han presentado ataques informáticos dos de nuestros clientes externos en su propia	Si, al momento de implementar no se despliega con políticas mínimas de seguridad	Si, las particiones de los sistemas operativos/aplicaciones se han quedado sin

	infraestructura presentando indisponibilidad del servicio. Es de resaltar que internamente a la fecha no se han presentado ataques internos.	de la información donde indica el cliente que se permite el acceso con el mismo usuario de manera simultánea.	espacio lo que ocasiona que los backup se ejecuten pero no se generen alertas al ser fallidos los procesos y en caso de restaurar la información afectaría su disponibilidad.
¿Tiene planeado realizar cambios en las políticas actuales para proteger la información de la empresa y clientes?	Si, en el momento se aplican políticas pero default de los aplicativos. No se cuenta con un diseño ni estrategia de Gestión de Seguridad Informática, siendo importante iniciar con el proceso para su planificación.	Desde mi área no realizamos cambios en las políticas de seguridad de la información, peso si son necesarias para el cliente externo.	Se deben realizar cambios y hay unos requerimientos con el director de tecnología, para su aplicación deben ser primero aprobados y certificados en ambientes de pruebas para verificar que no se presente afectación en sistemas operativos o aplicaciones.
¿Cuál es el mayor problema presentado por no contar con un Sistema de Gestión de	El mayor problema es al momento de renovación de contratos con los clientes donde	El mayor problema es al momento de ofrecer y presentar el producto a los clientes donde lo	Se ha presentado borrado de logs y al manejar el personal de soporte el super usuario

Seguridad de la Información?	prácticamente nos solicita como requisito tener las certificación en ISO 27001y por ende disponer un Sistema de Gestión de Seguridad de la Información.	primero que preguntan es por las políticas de seguridad de la información indicando que es un requisito para el proceso de contratación.	es difícil conocer quien ocasionó la novedad.
¿Cómo le gustaría que funcionara el Sistema de Gestión de Seguridad de la Información?	La forma de funcionar correctamente el Sistema de Gestión de Seguridad de la Información es donde no se afecten de manera negativa los actuales procesos de la empresa para evitar afectaciones a nivel de tiempo y costos.	Me gustaría que todos los aplicativos y ambientes cuenten con cada una de las políticas establecidas en los Sistemas de Gestión de Seguridad de la Información para brindar tranquilidad a los clientes.	Desde la infraestructura dar prioridad a las vulnerabilidades diseñando un plan de pruebas para garantizar siempre la disponibilidad del servicio.

Nota. La tabla presenta el resumen de las respuestas más imporantes de las entrevistas realizadas a los líderes del área de tecnología de AyA. Elaboración propia.

Análisis de los resultados de las entrevistas

Al realizar el análisis de las entrevistas se percibe la necesidad de implementar políticas de seguridad de la información a nivel de servidores, aplicativos y accesos lógicos y físicos,

siendo conscientes que la empresa AyA debe brindar la soluciones para una estrategia del Sistema de Gestión de Seguridad de la Información para contrarrestar las quejas del cliente externo donde el mismo cliente interno conoce las debilidades pero hasta el momento no se ha brindado solución oportuna de los hallazgos e inconformidades siendo prescindible para los clientes al momento de la renovación de contratos donde ven necesario que la empresa se certifique en la ISO 27001 para garantizar la seguridad de la información.

Internamente se han presentado novedades a nivel de consistencia de carpetas de aplicativos /sistemas operativos donde es imperioso la aplicación de políticas de acceso a servidores.

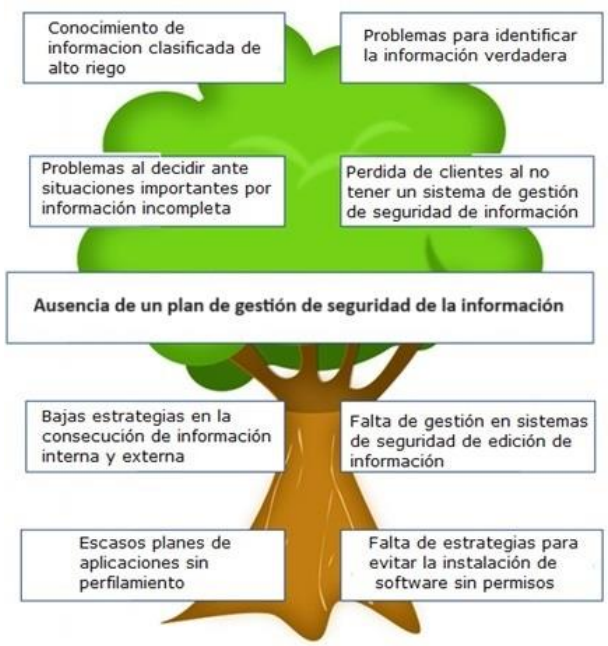
En cuanto a realizar cambios en las políticas actuales de seguridad se han presentado de manera independiente por los jefes de área al director de tecnología sin constituirse un documento unificado que englobe un SGSI indicando como les gustará que funcionara en la empresa donde es importante analizar que no se presenten reprocesos y por ende afectaciones a nivel de tiempo y costos, reconociendo la debilidad actual de riesgo de fuga de perdida de información al no contar con un Sistema de Gestión de Seguridad de la Información.

A su vez dentro de las debilidades se ve la necesidad de brindar a los actuales y futuros clientes confianza al resguardar la data bajo políticas de seguridad de la información mejorando los procesos tecnológicos en la organización.

Con base en el análisis de las respuestas se representa por medio del árbol de problemas para conocer las causas y efectos del problema.

Figura 7

Árbol de problemas análisis de resultados



Nota. El arból de problemas presenta la pregunta problema de estudio con sus principales causas y consecuencias. Elaboración propia.

Realizando el análisis del árbol de problemas la necesidad de una estrategia de Gestión de Seguridad de la Información surge ante el temor de los clientes de perdida de información e interiormente las sanciones económicas a generarse ante el no cumplimiento de la Ley 1581 de 2012 de protección de datos.

La falta de controles adecuados puede resultar en la divulgación no autorizada de información confidencial generando graves consecuencias para la reputación y la competitividad de la empresa al estar datos expuestos, los datos afectando la confiabilidad de la información

crítica para la toma de decisiones siendo vulnerables a ataques cibernéticos afectando la continuidad del negocio, resultando en costos significativos relacionados con la recuperación de datos, la investigación forense, las multas regulatorias y las demandas de clientes afectados quienes perciben a la empresa desorganizada en términos de seguridad afectando las relaciones comerciales e internamente la falta de un enfoque estructurado de la gestión de la seguridad de la información podría llevar a una falta de conciencia de seguridad entre los colaboradores de AyA aumentando el riesgo de errores humanos al disponer y manipular la información.

Creación del instrumento para aplicar la encuesta

Con la finalidad de profundizar en la problemática de estudio se requiere conocer la opinión de los colaboradores de la empresa referente al problema principal “Ausencia de una estrategia de gestión de seguridad de la información”

Las preguntas para la creación de las encuestas se plasman mediante el mapa de empatía

¿Qué Piensa y Siente?

1. ¿Actualmente la empresa cuenta con las políticas de seguridad para proteger el acceso a las aplicaciones? Selecciona una o varias opciones.

Las URL sólo están habilitadas para usuarios autorizados.

No se utilizan usuarios genéricos.

Las sesiones de usuario cuentan con políticas de inactividad.

Ninguna de las anteriores.

¿Qué Oye?

2. ¿Actualmente se cuenta con políticas de restauración de copias de respaldo?

Se ejecutan quincenalmente.

Se ejecutan mensualmente.

Se restauran copias sólo cuando es necesario.

No se restauran copias de seguridad.

3. ¿Actualmente hay establecidas políticas de acceso físico a las oficinas?

El acceso sólo habilita en horario hábil.

Se ingresa en cualquier horario.

No se cuenta con controles de acceso biométrico.

No tengo huella autorizada para ingresar a las oficinas.

4. ¿En cuáles secciones considera se deben aplicar controles de seguridad?

Personas.

Organizacional.

Tecnológicos.

Físicos.

Otros.

¿Qué Ve?

5. Al presentarse un incidente de seguridad se tiene un establecido (Seleccione una o varias respuestas):

Un plan y preparación para incidentes de seguridad.

Detección y análisis de incidentes.

Contención y erradicación de incidentes.

Ninguna de las anteriores.

6. ¿Al transferir la información cual tipo de cifrado utiliza?

Cifrado simétrico.

Cifrado asimétrico.

No utiliza cifrado.

¿Qué Dice y Hace?

7 ¿Al enviar un correo electrónico lo clasifica cómo?

Confidencial.

Restringido.

Uso Interno.

Público.

No clasifico el correo.

8. ¿Cuáles amenazas o ataques informáticos tiene conocimiento se ha presentado en la empresa?

Recepción de correos de cuentas desconocidas.

Correos con adjuntos sospechosos.

Denegación de servicio.

No tiene conocimiento de amenazas o ataques.

Esfuerzos

9. ¿En su rol en la compañía sabe cómo garantizar?

La confidencialidad de la información.

La integridad de la información.

La disponibilidad de la información.

No tengo el conocimiento.

Resultados

10 ¿Al certificarse en la ISO 27001 cuáles serían los beneficios para la empresa?

Coordinar los procesos de seguridad internos.

Ofrecer productos y servicios de calidad.

Mitigar los riesgos de seguridad.

Generar confianza entre los miembros de la organización.

11. ¿En cuánto considera que mejoraría la imagen de la empresa al implementar un Sistema de Gestión?

4 -Mejoraría bastante.

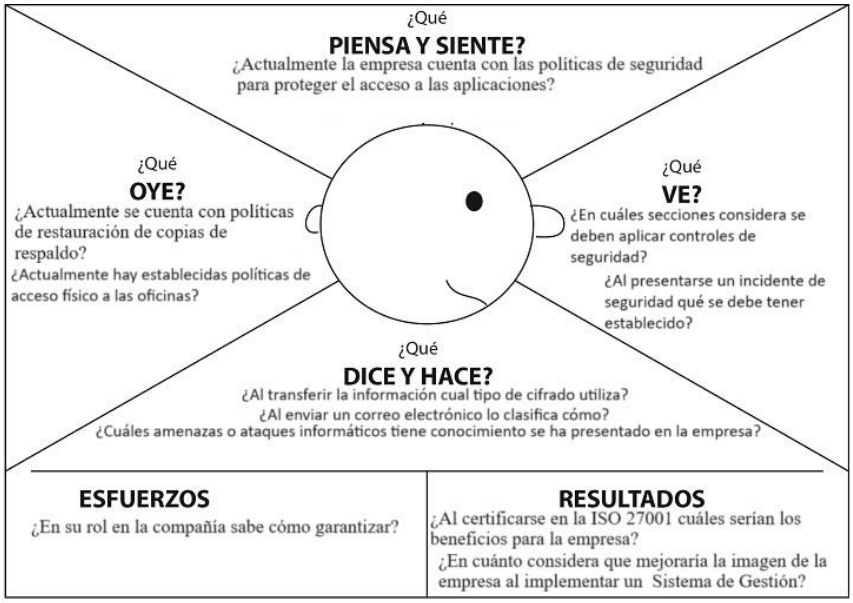
3 - Si Mejoraría.

2 -Mejoraría muy poco.

1- No mejoraría.

Figura 8

Mapa de Empatía preguntas encuestas



Nota. La figura muestra las preguntas a realizar en las encuestas por medio del mapa de empatía para conocer los problemas, deseos y demandas actuales de la seguridad de la información. Elaboración propia.

Determinación de Tamaño de la Muestra

La población estudiada oscila entre los 20 a 50 años quienes son los involucrados en el Sistema de Gestión de Seguridad de la Información.

El tamaño de la muestra se determina el nivel de confianza del 95%, tamaño de la población es de 30 personas, con un margen de error del 5%, dando como resultado el tamaño ideal de la muestra de 28 personas.

El lugar de desarrollo de la investigación son las oficinas de AyA ubicadas en la ciudad de Cali.

Tamaño de Muestra = Z2 * (p) * (1-p) / c2

Z = Nivel de confianza

P = Población

C = Margen de error

Aplicación de la encuesta a los colaboradores de la empresa AyA

La aplicación de la encuesta a los colaboradores de la empresa AyA se realiza mediante la herramienta Google Forms.

https://docs.google.com/forms/d/e/1FAIpQLSdUUCoGWyKwhWt4BzKZethg8DvKb-4_Cs5YNWGLHyy9WpE-LA/viewform?usp=sharing

La encuesta se realiza tomando como referencia el mapa de empatía tabulando los resultados en la herramienta Excel realizando preguntas cerradas para contrarrestar los márgenes de error.

La finalidad de la encuesta es conocer la opinión de los encuestados las cuales permitan un mayor análisis de la problemática de estudio que permite conocer las debilidades de seguridad que conlleven a la estrategia de Gestión de Seguridad de la Información.

Análisis de la encuesta realizada a los colaboradores de la empresa AyA

Las encuestas realizadas se tabulan en las herramientas Google Forms y Microsoft Excel para representar la opinión de los colaboradores. (Apéndice D).

Los resultados de las encuestas se visualizan en el Apéndice E para conocer las debilidades actuales ante la ausencia de una estrategia de Gestión de Seguridad de la Información.

A su vez por medio del Mapa de Empatía (Figura 16. *Mapa de empatía análisis encuesta*) se observan los resultados generales de las encuestas identificando:

El 77% de los colaboradores encuestados piensan y sienten que sólo la política de inactividad de sesiones de usuario se está utilizando parar proteger el acceso a las aplicaciones.

Igualmente oyen que no se están restaurando copias de seguridad. Sólo se restauran cuando es necesario ya sea por solicitud del director de tecnología, expresó el 90% de los encuestados.

A su vez referente a políticas de control de acceso físico a las oficinas de la compañía el ingreso y egreso se puede realizar a cualquier hora y día, según lo indicó el 90%, donde un 2% en el momento no cuenta con permisos de acceso.

Sobre los controles de seguridad que se requieren implementar en la empresa se resalta el tecnológico con un 75% y sólo un 5% considera importante contar con controles organizacionales.

Al presentarse un incidente de seguridad los colaboren ven en un 34% sólo se tiene establecido la contención y erradicación de incidentes y sólo un 32% indica que ay un plan de preparación de incidentes de seguridad.

Igualmente al momento de transferir información un 98% expresa que no utiliza ningún tipo de cifrado de la información.

Al enviar un correo electrónico el 70% dice que no clasifica el asunto del correo y sólo un 6% lo clasifica como confidencial.

Y sobre los ataques informáticos que se han presentado en la organización el 77% expresa que si ha recibido correos de remitentes desconocidos.

Referente al esfuerzo que cada colaborador debería hacer dentro de su rol para salvaguardar la seguridad de la información el 82% no tiene conocimiento de cómo garantizar la confidencialidad, disponibilidad e integridad de la información.

Y el resultado de certificarse en la ISO 27001 de Seguridad de la Información el 58% considera que sería ofrecer productos y servicios de calidad y el 98% cree que contar con un Sistema de Gestión de Seguridad de la información mejoraría bastante la imagen de la empresa.

Figura 9

Mapa de empatía análisis encuesta

*Nota***.** El mapa de empatía presenta el análisis de las encuestas detallando los porcentajes de los problemas y necesidades de los colaboradores referente a la seguridad de la información. Elaboración propia.

En las preguntas realizadas a los colaboradores de la empresa AyA se observa falta de controles y políticas para garantizar la seguridad de la información.

Los resultados demuestran que los colaboradores están en la disposición de participar en el sistema de gestión de seguridad de la información pero no sabe cómo hacerlo desde su rol en

la empresa pero es consciente que su implementación mejoraría procesos actuales y aumentaría la imagen de la empresa para el cliente interno y externo al dar el paso para la certificación en la ISO 27001 del SGSI.

Análisis las variables de carácter utilizando la matriz de identificación de problemas para validar las causas y efectos posteriormente con el árbol de problemas

La matriz de identificación de problemas se consolidan los problemas de objeto de estudio los cuales son el insumo de la solución o remediación de la situación actual tal como se observan en la tabla 3 (*Matriz de identificación de problemas*) donde se identifican problemas contractuales del el cual cliente solicita como requisito para renovar el contrato que la empresa cuente con un Sistema de Gestión de Seguridad de la Información, igual novedad se presenta al momento de ofrecer productos y servicios a nuevos clientes. De parte de los colaboradores desean participar en el SGSI pero desconocen cómo hacerlo desde su rol en la empresa.

Tabla 2

Matriz de identificación de problemas

INVOLUCRADO	**PROBLEMA**
Director de tecnología	Problemas contractuales al no contar con un sistema de gestión de seguridad de la información.
Jefe de implementación	Al capacitar nuevos clientes preguntan si está implementado el SGSI.
Jefe de Infraestructura	Al presentarse incidentes de seguridad no existe un plan de mitigación.
Colaboradores	Desde su rol no desconoce como garantizar la seguridad de la información.

Nota. La matriz de identificación de problemas muestra los problemas de mayor relevancia para los líderes de tecnología y colaboradores de la empresa AyA. Elaboración propia.

El árbol de problemas se representa gráficamente el resultado de las entrevistas realizadas al director de tecnología y jefes de área y encuestas realizadas a los colaboradores con la

finalidad de analizar causas y efectos al no contar con un Sistema de Gestión de Seguridad de la Información donde el problema principal es “el riesgo de no contar con un SGSI” teniendo como efecto “el riesgo de pérdida de la información” generando perdida de clientes, si no se cuenta con un plan de mitigación se puede presentar denegación del servicio, al no estar certificado en la ISO 27001 la empresa puede presentar problemas en la reputación empresarial y si los colaboradores de la empresa no saben cómo participar en el diseño y ejecución del SGSI y sus políticas se pueden desarrollar productos y servicios de baja calidad

Figura 10

Árbol de problemas de la matriz de identificación

Nota. El Árbol de problemas muestra el problema principal obtenido de las encuestas y entrevistas, sus causas y efectos al no contar con un sistema de seguridad de la información. Elaboración propia.

Síntesis del diagnóstico integral

En el diagnóstico se realizó entrevistas semiestructuradas al director de tecnología y jefes de área donde se conocieron los problemas y debilidades presentes al no contar con un Sistema de Gestión de Seguridad de la Información, conglomerando la información en un árbol de problema para identificar el problema principal y sus causas y efectos.

Se realizaron encuestas a los 30 colaboradores analizando los resultados en la herramienta mapa de empatía resaltando en un 82% el interés del personal en colaborar con el SGSI desde su rol en la empresa para mejorar la calidad de productos y servicios.

Cada área de la empresa indicó desde su campo de acción cual es el problema de mayor afectación unificando la información en una Matriz de identificación de problemas.

Determinar las posibles soluciones de la estrategia de un Sistema de Gestión de Seguridad de la Información (SGSI)

En la fase de tratamiento se realiza el análisis del diagnóstico y selección de las posibles soluciones para diseñar la estrategia del Sistema de Gestión de Seguridad de la Información a partir de cuadros comparativos.

Análisis del diagnóstico integral mediante la matriz DOFA extendida

Se diseña la Matriz DOFA extendida del diagnóstico integral (Tabla 3. Matriz DOFA del diagnóstico integral) analizar el diagnóstico integral de las encuestas realizada a los colaboradores de la empresa AyA. En el prime campo se describe la problemática actual de estudio la cual origina el caso de estudio.

El campo Fortalezas presenta a los aspectos positivos y ventajas competitivas del diagnóstico de la estrategia del Sistema de Gestión de Seguridad de la Información en la empresa AyA.

El campo Debilidades hace referencia a las limitaciones y desventajas que pueden afectar la capacidad para alcanzar los objetivos del SGSI para poder desarrollar estrategias de mitigación de obstáculos.

El Campo Estrategias FO indica los enfoques que se pueden adoptar para aprovechar sus Fortalezas y las Oportunidades maximizando el rendimiento y la posición competitiva al abordar los puntos fuertes.

El campo Estrategias DO muestra a las acciones y enfoques para superar sus Debilidades y aprovechar las Oportunidades mejorando los puntos más débiles del SGSI para convertir debilidades en fortalezas.

El campo Oportunidades presenta los factores positivos y favorables para alcanzar los objetivos comprendiendo que oportunidades permiten desarrollar y obtener beneficios.

El campo Amenazas detalla las situaciones desfavorables que representar riesgos para el SGSI. Al identificar las amenazas se desarrollan estrategias efectivas para mitigar su impacto.

El campo Estrategias FA explica se refiere a las acciones a adoptar para aprovechar las fortalezas internas y enfrentar las amenazas externas.

El campo Estrategias DA adopta las acciones para mitigar las Debilidades internas y enfrentar las Amenazas externas para minimizar riesgos y desafíos externos que pueden agravar las debilidades.

Tabla 3

Matriz DOFA del diagnóstico integral

DESCRIPCIÓN DEL PROBLEMA	FORTALEZAS	DEBILIDADES
Es necesario planear un sistema de gestión de seguridad de la información para garantizar la seguridad de los activos de la empresa que son software e información la cual debe garantizar la disponibilidad de manera segura y para el personal autorizado con la finalidad de mostrar una mayor imagen de confianza del cliente interno y externo, dando el valor agregado de credibilidad por lo cual se aplicarán técnicas herramienta como el árbol de problemas y mapa de empatía para seleccionar la mejor estrategia. Si la empresa AyA contará con un sistema de gestión de seguridad de la información puede agilizar y gestionar procesos de manera segura ,y de esta manera preparar al personal para certificarse, lo cual es una ventana para mantener clientes satisfechos al ver que su información está protegida y a su vez es una entrada a nuevos clientes quienes al momento de compartir el activo más importante de cualquier empresa la información lo hacen en medio de la desconfianza y la precaución, y la certificación en seguridad de la información es la puerta de transacciones seguras donde cada bit será protegido.	Promover la confidencialidad, integridad y disponibilidad de la información. Mejora en las instalaciones físicas. Transferencia de conocimiento actualizado. Integración de procesos. Rigurosidad técnica. Reducción de riesgos en la interrupcion del servicio. Mejora en el nivel de satisfacción del cliente.	Desconocimento de la metodología para implementar un SGSI. La empresa carece de monitoreo y seguimiento de las politcas implementadas actualmente. Sensibilizar al cliente externo en el SGSI. No se dispone de un plan de respuesta a incidentes. No se realizan auditorías de seguridad.

OPORTUNIDADES	ESTRATEGIAS FO	ESTRATEGIAS DO
Fortalecer los planes de mejora contínua. Fortalecer los sistemas de información. Garantizar el buen uso de la tecnología. Contar con recursos económicos para el SGSI. Implementar las políticas de seguridad de la información. Apertura de nuevos mercados. Atraer nuevos inversionistas. Certificación en la ISO 27001. Aumentar la confianza interna en la empresa.	Capitalizar las fortalezas tecnológicas existentes para adoptar nuevas tecnologías y mejorar la eficiencia. Establecer alianzas estratégicas con empresas innovadoras para aprovechar oportunidades de colaboración. Utilizar las fortalezas de la organización para cumplir con normativas y estándares, mejorando así la reputación. Utilizar las fortalezas existentes para expandir las operaciones a nivel global y aprovechar nuevas oportunidades de mercado. Reforzar la cultura de seguridad mediante programas de concienciación para capitalizar las oportunidades de mejora. Utilizar el equipo altamente calificado para desarrollar e implementar medidas de seguridad avanzadas.	Desarrollar y poner en práctica procedimientos efectivos de respuesta a incidentes para abordar las debilidades en la gestión de incidentes. Mejora en la cultura organizacional de la empresa.

	Continuar invirtiendo en la modernización de la infraestructura tecnológica para mantener la competitividad. Utilizar la eficiencia en la gestión de incidentes como una ventaja competitiva y ofrecer servicios de respuesta a incidentes a otras organizaciones..	
AMENAZAS	**ESTRATEGIAS FA**	**ESTRATEGIAS DA**
Dificultad al momento de implementar las políticas. Falta de compromiso de la gerencia para implementar el SGSI. Oposición interna en la implementación. Ataques informáticos mientras se crea la estrategia del SGSI. Obsolencencia tecnológica. Falta de un plan de contingencia. Malas practicas en el uso de herramientas tecnológicas. Falta de políticas de seguridad. Retraso en las contrataciones. Falta de recursos económicos.	Mejorar las fortalezas organizativas para enfrentar la competencia en el mercado y destacar en términos de seguridad.	Establecer un plan de actualización tecnológica para contrarrestar las amenazas asociadas con la obsolescencia. Reforzar las medidas de seguridad cibernética y establecer planes de contingencia para mitigar los ciberataques. Monitorear activamente los cambios legislativos y trabajar para cumplir con nuevas regulaciones. Desarrollar planes de contingencia y recuperación ante desastres para abordar

amenazas de eventos naturales.

Nota. La gráfica permite analizar el diagnóstico integral de las encuestas realizada a los colaboradores de la empresa AyA, por medio de la matriz Dofa extendida. Elaboración propia.

La matriz DOFA muestra las debilidades, fortalezas, oportunidades y amenazas unificando conceptos y opiniones de las entrevistas y encuestas realizadas, donde de las debilidades se presentan las mejoras del caso en estudio.

En cuanto a las fortalezas del Sistema de Gestión de Seguridad de la Información mejoraría la cultura organizacional de la empresa al promover la confidencialidad, integridad, disponibilidad de la información reduciendo los riesgos de perdida de información e interrupción de los servicios prestados a terceros aumentando el nivel de satisfacción de los clientes, destacando las oportunidades para fortaleciendo al personal por medio de capacitaciones optimizando los planes de mejora continua garantizando el buen uso de la tecnología en especial de los sistemas de información y así aprovechar todas las oportunidades para certificarse en la ISO27001 al contar con un sistema de gestión de seguridad de la Información atrayendo nuevos inversionistas y aperturando nuevos mercados.

Al identificar las fortalezas de la estrategia del Sistema de Gestión de Seguridad de la Información (SGSI) es importante la existencia de políticas sólidas, personal capacitado y sistemas robustos.

Al conocer las debilidades se perciben lagunas en las políticas de seguridad establecidas, falta de conciencia de seguridad entre el personal y sistemas de seguridad desactualizados.

Al validar las estrategias FO es importante la mejora continua de los controles de seguridad existentes adoptando nuevas tecnologías de seguridad y compartir las buenas prácticas para fortalecer la seguridad de la información.

Al analizar las Estrategias DO se incluyen procedimientos de respuesta a incidentes para fortalecer los controles de seguridad débiles para abordar las amenazas cibernéticas.

En las Oportunidades se deben implementar tecnologías avanzadas de seguridad acorde a los cambios regulatorios por hallazgos, vulnerabilidades o actualizaciones en la normatividad.

En las amenazas se destacan la pérdida o robo de datos, la interrupción del servicio y la exposición a sanciones legales por incumplimiento de normativas de seguridad.

En las estrategias FA es importante el fortalecimiento de controles de seguridad en áreas identificadas como fortalezas y estar preparados para la adaptación proactiva a cambios en las regulaciones de seguridad de la información.

En las estrategias DA se considera indispensable contar con expertos internos y externos en ciberseguridad para fortalecer las defensas ante amenazas cibernéticas.

Síntesis de las alternativas de solución para el Sistema de Gestión de Seguridad de la Información

En las alternativas para el Sistema de Gestión de Seguridad de la Información la primera condición es obtener el compromiso activo de la alta dirección para respaldar la implementación y mantenimiento del SGSI y así realizar un análisis de riesgos para identificar y evaluar las amenazas y vulnerabilidades que afectan la seguridad de la información para establecer claramente el alcance del SGSI, incluyendo activos, procesos y áreas de la organización que deben ser cubiertas desarrollando políticas y procedimientos de seguridad de la información que reflejen los objetivos y requisitos de la empresa AyA para implementar controles técnicos y

organizativos para mitigar los riesgos de seguridad identificados durante el análisis y para ello es importante realizar auditorías internas y revisiones periódicas del SGSI para asegurar su conformidad y eficacia continua, de esta manera comprometerse con la mejora continua del SGSI a través de la revisión regular de políticas, procedimientos y controles, estableciendo métricas y KPIs para medir el desempeño del SGSI y la eficacia de los controles implementados. Y con el resultado de las revisiones proporcionar formación en seguridad de la información a todos los empleados para fomentar una cultura de seguridad.

Estas condiciones son fundamentales para establecer y mantener un SGSI sólido que proteja la información de la organización y garantice su integridad, confidencialidad y disponibilidad.

Definir los criterios técnicos de las posibles estrategias del Sistema de Gestión de Seguridad de la Información por medio de un cuadro comparativo

En el momento se requiere un Sistema de Gestión de Seguridad de la Información en la empresa siendo de vital importancia para la gerencia y dirección de tecnología para tener productos y servicios de calidad y mejorar los procesos tecnológicos internos garantizando su ejecución de manera segura.

En el cuadro comparativo se realizará el análisis de varios modelos de sistemas gestión de seguridad de la información para seleccionar el modelo más adecuado según las necesidades expresadas por colaboradores y líderes de procesos.

El cuadro comparativo *de* modelos de SGSI (Tabla 5. *Cuadro comparativo de estrategias de SGSI*) presenta las diversas estrategias del sistemas de gestión de seguridad de la información para su análisis donde para conocer y seleccionar el más acorde para la empresa es importante analizar los aspectos de enfoque principal del sistema, además del alcance dentro de la

organización y sus procesos, al conocer la estructura se valida las bases sobre el cual está construido el modelo y así detallar los riesgos que cubre, de igual manera por medio de la flexibilidad validar el nivel de adaptación, en cuanto a la certificación saber cuál ofrece mayor cobertura sobre políticas de seguridad de la información, igualmente conocer el enfoque de continuidad del negocio.

Tabla 4

Cuadro comparativo de alternativas de SGSI

ASPECTO	OSSTMM 3	NIST	COBIT 5	ISO 27001
Enfoque Principal	Pruebas de seguridad.	Directrices de seguridad.	Gobierno y gestión de TI.	Gestión de seguridad de la información.
Alcance	Evaluación de vulnerabilidades y amenazas. Centrado en pruebas de seguridad y evaluación de riesgos.	Guías y Ofrece directrices y recomendaciones para mejorar la seguridad de la información y la ciberseguridad.	Gobierno de TI y gestión de riesgos. Enfocado en gobierno y gestión de TI, incluyendo la alineación con los objetivos del negocio.	Implementación de un sistema de gestión de seguridad de la información. Se enfoca en la seguridad de la información y establece requisitos para un sistema de gestión de seguridad de la información (SGSI).
Estructura	Proporciona un conjunto de metodologías y procedimientos para realizar pruebas de seguridad de la información.	Proporciona una serie de publicaciones, como el marco de ciberseguridad NIST y el marco de gestión de riesgos NIST, con pautas detalladas.	Ofrece un marco de referencia en forma de procesos y dominios, con objetivos de control y prácticas recomendadas.	Establece un sistema de gestión de seguridad de la información (SGSI) con un enfoque basado en el ciclo Planificar-Hacer-Verificar-Actuar (PDCA).
Enfoque de riesgos	Se centra en la evaluación y prueba de riesgos específicos de seguridad.	Aborda la gestión de riesgos en la ciberseguridad, pero no se enfoca	Incluye una perspectiva de riesgo pero se centra en la gestión	Requiere una evaluación de riesgos y tratamiento de

		exclusivamente en pruebas de seguridad.	de TI en general, no solo en la seguridad.	riesgos como parte integral del SGSI.
Flexibilidad	Se enfoca en pruebas de seguridad y evaluación de riesgos, con un enfoque específico.	Proporciona un enfoque más amplio para mejorar la seguridad de la información y la ciberseguridad.	Se adapta a las necesidades de la organización en cuanto a gobierno y gestión de TI.	Proporciona un marco general y se puede adaptar a diversas organizaciones y sectores.
Certificación	No ofrece certificación directa, pero proporciona una guía para pruebas de seguridad.	No emite certificaciones, pero sus directrices son ampliamente adoptadas en todo el mundo.	Ofrece certificaciones relacionadas con la gestión de TI y el gobierno de la empresa.	ISO 27001 proporciona una base para la certificación de sistemas de gestión de seguridad de la información (SGSI).
Proceso de Evaluación	Metodología de pruebas de seguridad con fases específicas.	Marco de gestión de riesgos (RMF) con etapas definidas.	Modelo de referencia con dominios y procesos.	Ciclo PDCA (Planificar, Hacer, Comprobar, Actuar).
Enfoque en Continuidad del Negocio	No	Parte de consideraciones de seguridad.	Parte de la gestión de riesgos.	Parte de la gestión de riesgos y la continuidad del negocio.

*Nota***.** La tabla muestra las características técnicas de las estrategias de los sistemas de gestión de seguridad de la información.

Análisis de las ventajas y desventajas de los criterios técnicos de los Sistema de Gestión de Seguridad de la Información

El Cuadro comparativo de estrategias de SGSI (Tabla 5. *Cuadro comparativo de estrategias de SGSI)* se utilizó para analizar las alternativas del sistema de gestión de seguridad

de la información para la empresa AyA, y de esta manera debatir cual sería la mejor opción para la estrategia del SGSI.

El cuadro comparativo permite analizar las estrategias del sistema de información OSSTMM 3, NIST, COBIT 5, ISO 27001, según los criterios de gestión de seguridad de la información para determinar las ventajas y desventajas presentes.

Dentro de las ventajas OSSTMM 3 proporciona un enfoque estructurado y detallado para realizar pruebas de seguridad de la información, lo que lo hace valioso para los profesionales de seguridad, al centrarse en la evaluación de riesgos permite a las organizaciones identificar y abordar las vulnerabilidades de manera más efectiva. Además es flexible para adaptarse a las necesidades específicas de las organizaciones haciéndolo adecuado para una variedad de entornos y situaciones.

Referente a las desventajas es menos conocido y menos ampliamente adoptado en comparación con otros marcos de seguridad de la información limitando su aceptación en ciertos entornos, además la disponibilidad de recursos, capacitación y documentación específica puede ser limitada en comparación con otros marcos más ampliamente utilizados.

Según (Rose, M., 2019) los estándares y guías de NIST son ampliamente aceptados a nivel internacional promoviendo un enfoque basado en riesgos para la seguridad de la información ayudando a las organizaciones a priorizar sus esfuerzos de seguridad de manera efectiva.

Igualmente proporciona una amplia gama de recursos abiertos y gratuitos incluyendo guías, herramientas y referencias que ayudan a las organizaciones en la mejora de su seguridad.

Sobre las desventajas los estándares de NIST son genéricos y pueden no abordar las necesidades específicas de ciertos sectores económicos. Su implementación puede requerir

tiempo y recursos significativos, lo que puede ser una desventaja para organizaciones con restricciones.

(Herold, D., 2015) a nivel de ventajas indica que el COBIT 5 se centra en la gobernanza y la gestión efectiva de la tecnología de la información en alineación con los objetivos del negocio ayudado a las organizaciones a optimizar sus recursos de TI, alineándose con estándares y marcos de referencia como ISO 27001 e ITIL, proporcionando un enfoque estructurado para medir el desempeño y la eficacia de las operaciones de TI facilitando la toma de decisiones basadas en datos.

Referente a las desventajas expresa que la implementación completa de COBIT 5 puede requerir recursos financieros considerables, incluida la formación y la contratación de personal especializado. Y la desventaja de mayor envergadura es que COBIT 5 es un marco general que no se enfoca en aspectos específicos de seguridad de la información o ciberseguridad requiriendo la integración con otros marcos o estándares.

Para (Van Der Heyden, J., 2015) dentro de las ventajas de la ISO 27001 está promover la implementación de controles de seguridad reduciendo el riesgo de incidentes de seguridad de la información, basada en un enfoque de gestión de riesgos ayudando a las organizaciones a identificar y abordar las amenazas de manera sistemática brindando una ventaja competitiva al demostrar su compromiso con la seguridad de la información.

La norma proporciona un marco estructurado y detallado para establecer y mantener un sistema de gestión de seguridad de la información (SGSI) facilitando la implementación y la gestión efectiva de la seguridad de la información.

En relación a las desventajas (Van Der Heyden, J., 2015) indica que la implementación y certificación de la ISO 27001 pueden ser complejas y costosas para organizaciones más

pequeñas, además la norma no es una solución única y requiere mantenimiento continuo para mantenerse actualizada. De otra parte la ISO 27001 enfatiza la documentación de políticas y procedimientos lo que puede generar una carga administrativa significativa.

Es importante enfatizar que la norma no proporciona detalles específicos sobre controles técnicos requiriendo la integración con otros estándares y marcos.

Calificación de las alternativas de los sistemas de seguridad de la información utilizando la matriz de ponderación técnica

La matriz de ponderación técnica (Tabla 5. *Matriz de ponderación técnica)* para validar y dar una calificación a cada una de las características de modelos y/o estándares de seguridad de la información.

El encargado de calificar las características de cada modelo es el director de tecnología quien es la persona encargada de seleccionar y autorizar los cambios a nivel de software, hardware y procesos tecnológicos en la empresa AyA

Dentro de las características a calificar se encuentran enfoque principal, alcance, estructura, enfoque de riesgos, flexibilidad, certificación y enfoque de continuidad del negocio.

La calificación de cada aspecto es de 1 a 10 donde 1 es la calificación más baja y 10 la calificación más alta.

Tabla 5

Matriz de ponderación técnica

ASPECTO	**OSSTMM 3**	***Ptos***	**NIST**	***Ptos***	**COBIT 5**	***Ptos***	**ISO 27001**	***Ptos***
Enfoque Principal	Pruebas de seguridad.	1	Directrices de seguridad.	7	Gobierno y gestión de TI.	10	Gestión de seguridad de la información.	10
Alcance	Evaluación de vulnerabilidades y amenazas. Centrado en pruebas de seguridad y evaluación de riesgos.	5	Guías y Ofrece directrices y recomendaciones para mejorar la seguridad de la información y la ciberseguridad.	7	Gobierno de TI y gestión de riesgos. Enfocado en gobierno y gestión de TI, incluyendo la alineación con los objetivos del negocio.	8	Implementación de un sistema de gestión de seguridad de la información. Se enfoca en la seguridad de la información y establece requisitos para un sistema de gestión de seguridad de la información (SGSI).	10

Estructura	Proporciona un conjunto de metodologías y procedimientos para realizar pruebas de seguridad de la información.	8	Proporciona una serie de publicaciones, como el marco de ciberseguridad NIST y el marco de gestión de riesgos NIST, con pautas detalladas.	7	Ofrece un marco de referencia en forma de procesos y dominios, con objetivos de control y prácticas recomendadas.	8	Establece un sistema de gestión de seguridad de la información (SGSI) con un enfoque basado en el ciclo Planificar-Hacer-Verificar-Actuar (PDCA).	10
Enfoque de riesgos	Se centra en la evaluación y prueba de riesgos específicos de seguridad.	6	Aborda la gestión de riesgos en la ciberseguridad, pero no se enfoca exclusivamente en pruebas de seguridad.	6	Incluye una perspectiva de riesgo pero se centra en la gestión de TI en general, no solo en la seguridad.	9	Requiere una evaluación de riesgos y tratamiento de riesgos como parte integral del SGSI.	9
Flexibilidad	Se enfoca en pruebas de seguridad y evaluación de riesgos,	5	Proporciona un enfoque más amplio para mejorar la seguridad de la	9	Se adapta a las necesidades de la organización en cuanto	9	Proporciona un marco general y se puede adaptar a diversas	9

	con un enfoque específico.		información y la ciberseguridad		a gobierno y gestión de TI.		organizaciones y sectores.	
Certificación	No ofrece certificación directa, pero proporciona una guía para pruebas de seguridad.	1	No emite certificaciones, pero sus directrices son ampliamente adoptadas en todo el mundo.	1	Ofrece certificaciones relacionadas con la gestión de TI y el gobierno de la empresa.	10	ISO 27001 proporciona una base para la certificación de sistemas de gestión de seguridad de la información (SGSI).	10
Proceso de Evaluación	Metodología de pruebas de seguridad con fases específicas.	3	Marco de gestión de riesgos (RMF) con etapas definidas.	7	Modelo de referencia con dominios y procesos.	9	Ciclo PDCA (Planificar, Hacer, Comprobar, Actuar).	9
Enfoque en Continuidad del Negocio	No	1	Parte de consideraciones de seguridad.	6	Parte de la gestión de riesgos.	8	Parte de la gestión de riesgos y la continuidad del negocio.	8
Total		30		50		71		75

Nota. La tabla de ponderación técnica otorga calificación a cada item de los sistemas de seguridad de la información para preseleccionar los más acordes a las necesidades de la empresa.

Selección de acuerdo a los resultados obtenidos y en relación a los requerimientos y necesidades de la gerencia del pre- diseño de la estrategia del Sistema de Gestión de Seguridad de la Información (SGSI)

Los resultados obtenidos (Tabla 5. *Matriz de ponderación técnica)* indican que referente a los sistemas de seguridad de información las más baja calificación es para el modelo OSSTMM 3 con 30 puntos, NIST obtuvo una calificación de 50 puntos, COBIT 5 tiene una calificación de 71 puntos y la calificación más alta es para la ISO 27001 con 75 puntos, siento está ultima la opción más viable de acuerdo a la ponderación realizada por el director de tecnología

Por medio del cuadro comparativo se obtuvo una visión general sobre las necesidades de la empresa y los diversos modelos de seguridad de la información permitiendo seleccionar aquel que cumpla con los requerimientos técnicos y de calidad con la finalidad de crear la estrategia del Sistema de Gestión de Seguridad de la Información en la empresa AyA donde se puede garantizar la disponibilidad, confidencialidad e integridad de la información.

Síntesis de la fase de las alternativas de seguridad de la información

En la fase de tratamiento se diseñó la Matriz DOFA extendida del diagnóstico integral para realizar el análisis de los modelos para conocer las fortalezas y debilidades al momento de contar con una estrategia del SGSI.

Se conocieron técnicamente los modelos propuestos para el SGSI para posteriormente analizar sus ventajas y desventajas procediendo a calificar y seleccionar el modelo más acorde por la empresa AyA por medio de la Matriz de Ponderación Técnica (Tabla 5).

Consolidación de la información de las estrategias con las alternativas para la elaboración del SGSI y las políticas de Seguridad de la Información

Para determinar las posibles soluciones del del sistema de gestión de seguridad de la nformación por medio de las herramientas utilizadas tienen prioridad la calidad, seguridad y respuesta a incidentes seleccionando el modelo con más alta calificación.

Se conocieron opiniones de los diversos sistemas de seguridad de la información el cual puede cubrir los requerimientos donde se analizaron las estrategias OSSTMM 3, NIST, COBIT 5, ISO 27001 describiendo las características técnicas por medio de un cuadro comparativo donde se encontró que el Sistema de Gestión de Seguridad de la Información debe estar regido por los estándares de la norma ISO 27001 cumpliendo con las necesidades de la empresa.

Posteriormente mediante el cuadro comparativo (Tabla 5) se analizaron las ventajas y desventajas recolectando información para brindar una opinión acorde a los requerimientos de seguridad donde se analizaron estrategias de seguridad para optar la opción con los mayores criterios técnicos donde en la matriz de ponderación la calificación más alta la obtuvo el estándar

ISO27001 siendo seleccionada para diseñar la estrategia de gestión de seguridad de la información.

Herramienta C/B para establecer la mejor estrategia del Sistema de Gestión de Seguridad de la Información

La herramienta costo/beneficio de excel se utiliza para conocer los costos asociados de cada estrategia del Sistema de Gestión de Seguridad de la Información donde se toma como base la tasa del 8%. Cada estrategia se proyecta a 3 años el costo y beneficio que es el tiempo de vigencia de la certificación en seguridad de la información donde en el año cero está estipulado el valor del costo de la puesta en marcha del SGSI y la certificación, los siguientes años son de mantenimiento del sistema.

La fórmula utilizada es VNA (Valor Neto Actual) donde devuelve el valor neto presente de la inversión a partir de una tasa de descuento y pagos futuros.

La misma fórmula es utilizada para hallar el valor Presente de manera individual de Beneficios y Costos.

Se realiza la división del Valor Presente Beneficios y Valor Presente Costos para obtener el valor de la Relación de Costo Beneficio B/F.

Si B/C >1, los beneficios son superiores a los costos, la estrategia del Sistema de Gestión de Seguridad de la Información es viable.

Si B/C =1, no hay ganancias en el SGSI.

Si B/C <1, Los beneficios son inferiores a los costos, la estrategia del Sistema de Gestión de Seguridad de la Información no es viable.

Tabla 6

Costo/Beneficio tasa del 8%

PLAN 1. Plan del Sistema de Gestión de Seguridad de la Información OSSTMM 3	**Año 0**	**Año 1**	**Año 2**	**Año 3**	**Valor Presente**
Beneficios	$ 0	$ 1.500.000	$ 2.000.000	$ 3.000.000	$ 5.078.762,27
Costos	$ 7.000.000	$ 1.200.000	$ 1.000.000	$ 900.000	$ 8.965.647,17
	Relación Costo Beneficio B/F				$ 0,57
PLAN 2. Plan del Sistema de Gestión de Seguridad de la Información NIST	**Año 0**	**Año 1**	**Año 2**	**Año 3**	**Valor Presente**
Beneficios	$ 0	$ 1.800.000	$ 2.200.000	$ 3.200.000	$ 5.641.736,34
Costos	$ 7.000.000	$ 1.200.000	$ 1.000.000	$ 900.000	$ 8.965.647,17
	Relación Costo Beneficio C/B				**$ 0,63**
PLAN 3. Plan del Sistema de Gestión de Seguridad de la Información COBIT 5	**Año 0**	**Año 1**	**Año 2**	**Año 3**	**Valor Presente**
Beneficios	$ 0	$ 4.000.000	$ 5.000.000	$ 6.000.000	$ 11.808.695,60
Costos	$ 7.000.000	$ 1.200.000	$ 1.000.000	$ 900.000	$ 8.965.647,17
	Relación Costo Beneficio C/B				**$ 1,32**
PLAN 4. Plan del Sistema de Gestión de Seguridad de la Información ISO 27001	**Año 0**	**Año 1**	**Año 2**	**Año 3**	**Valor Presente**
Beneficios	$ 0	$ 5.000.000	$ 6.000.000	$ 7.000.000	$ 14.194.896,52
Costos	$ 7.000.000	$ 1.200.000	$ 1.000.000	$ 900.000	$ 8.965.647,17
	Relación Costo Beneficio C/B				**1,58**

Nota. La figura presenta la proyección a 4 años de los sistemas de seguridad de la información en relación al costo beneficio. Elaboración propia.

Al realizar el análisis Costo/Beneficio de Excel los SGSI sólo se tienen en cuenta aquellos donde la relación C/B es >1, al ser viables para la empresa AyA al retornar beneficios en un lapso de 3 años tiempo de vigencia de la certificación en seguridad de la información. Al terminar ese plazo se requiere iniciar todo el proceso para postularse a una nueva certificación.

La estrategia con la relación Costo/Beneficio es el modelo ISO27001 con una relación de 1,58 al generar los beneficios más altos en relación al costo al cumplir con mayores controles y

secciones de seguridad dentro del contexto de empresa como lo es el liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora continua. A diferencia del modelo COBIT 5 que sólo cubre los procesos de planificación, soporte, y monitoreo, lo cual generaría mayores costos y menos beneficios para la empresa al tratar de cubrir los ámbitos estipulados por la ISO 27001.

Selección de la mejor estrategia del Sistema de Gestión de Seguridad de la Información

En la empresa AyA para establecer los controles del Sistema de Gestión de Seguridad de la Información se tomará como referencia la ISO 27001 donde es importante comprender los requisitos de seguridad de información para el establecimiento de objetivos y políticas con la finalidad de implementar controles para minimizar los riesgos de seguridad de la información garantizando la integridad disponibilidad, integridad y confidencialidad de la información por medio del del Sistema de Gestión de Seguridad de la Información (SGSI).

Para realizar la selección de la mejor estrategia se tuvo en cuenta las herramientas de cuadro comparativo, matriz de ponderación técnica y Costo Beneficio donde se tuvo en cuenta la mayor calificación y beneficio a 3 años.

Activos a proteger en el sistema de gestión de seguridad de la información

En la entrevista realizada al director de tecnología se determinaron los activos a proteger en la empresa relacionándolos en una tabla conocer el tipo de activo y sus especificaciones.

En la primera columna (Tabla 7. *Activos a proteger*) se indica el tipo de activo a proteger, en la segunda columna se muestra la descripción del activo y en la tercera columna se plantea la política de seguridad del activo a proteger.

Tabla 7

Activos a proteger

Tipo de Activo	Descripción	Especificaciones a Proteger
Información	Datos confidenciales	Acceso no autorizado. Divulgación no autorizada. Modificación no autorizada. Destrucción no autorizada.
Sistemas de información	Servidores	Acceso no autorizado. Información. Disponibilidad no autorizada. Configuraciones seguras. Copias de seguridad adecuadas. Protección contra malware y virus. Actualizaciones de software.
Redes	Equipos de red	Acceso no autorizado a la red. Monitoreo y detección de intrusiones. Configuraciones seguras de red.

		Control de acceso a la red. Protección contra ataques de denegación de servicio.
Instalaciones	Centro de datos	Acceso físico restringido. Seguridad contra incendios y desastres. Sistemas de control de acceso físico. Respaldo de energía eléctrica.
Personal	Empleados	Procedimientos de contratación seguros. Formación en seguridad de la información. Políticas de uso aceptable. Control de acceso a la información. Procedimientos de terminación seguros. Gestión de identidad y accesos. Concienciación sobre seguridad de la información.
Equipos	Computadores y dispositivos	Controles de acceso físico y lógico. Encriptación de datos sensibles. Políticas de uso de dispositivos. Actualizaciones y parches de seguridad. Respaldo y recuperación de datos.

*Nota***.** La tabla explica los activos que requiere proteger la empresa sobre los cuales se diseñarán las políticas de seguridad de la información.

A nivel de la información es importante proteger los datos confidenciales, como información financiera, datos de clientes, propiedad intelectual. Teniendo en cuenta el acceso no autorizado garantizando que solo personal autorizado tenga acceso a la información. Evitar la divulgación no autorizada, modificación no autorizada, destrucción no autorizada, clasificando y etiquetado la información para garantizar la integridad y confidencialidad.

En los Sistemas de Información se deben proteger servidores, bases de datos, sistemas operativos y aplicaciones de acceso no autorizado a sistemas por medio de configuraciones seguras para prevenir vulnerabilidades garantizando la protección contra malware y virus al mantener los sistemas actualizados.

En las redes se deben proteger los equipos de red, routers, switches, firewalls de acceso no autorizado monitoreando y detectando intrusiones, y en especial ataques de denegación de servicio por medio de controles de acceso a la red.

En las instalaciones se requiere proteger centros de datos, oficinas, salas de servidores garantizando acceso físico, seguridad contra incendios y desastres, respaldo de energía eléctrica para no afectar la continuidad del negocio.

El tipo de activo Personal hace referencia a empleados, contratistas y socios comerciales donde es importante verificar antecedentes y referencias, además de capacitarlos en seguridad de

la información para establecer el uso de los recursos de información limitando el acceso solo a la información necesaria para las funciones laborales.

Los equipos a proteger son computadoras, dispositivos móviles, impresoras de acceso no autorizado encriptando datos sensibles estableciendo reglas para el uso de equipos además de actualizar los sistemas de información para protegerlos contra malware y virus garantizando la disponibilidad y recuperación de la información.

Esta clasificación y especificación son esenciales para diseñar e implementar controles de seguridad adecuados en un SGSI y para garantizar la protección de los activos críticos de la organización.

Documentación necesaria para establecer la mejor estrategia del Sistema de Gestión de Seguridad de la Información

La norma ISO/IEC 27001 establece requisitos específicos de documentación para la estrategia de un sistema de gestión de seguridad de la información.

Política de Seguridad de la Información (PSI)

La empresa debe establecer y mantener una política de seguridad de la información.

Alcance del SGSI

Definir y documentar el alcance del SGSI identificando los límites y aplicabilidad del sistema.

Proceso de Evaluación de Riesgos y Tratamiento

Debe documentarse el proceso para la evaluación de riesgos y la determinación de los controles de seguridad aplicables.

Declaración de Aplicabilidad

La empresa debe documentar una Declaración de Aplicabilidad que especifique los controles de seguridad seleccionados y justifique su implementación.

Políticas y Procedimientos de Seguridad

Se requiere establecer y documentar políticas y procedimientos de seguridad de la información para implementar los controles seleccionados.

Roles y Responsabilidades

La empresa debe definir y documentar roles, responsabilidades y autoridades para la gestión de la seguridad de la información.

Concientización, Capacitación y Competencia

Debe existir documentación relacionada con la concientización, capacitación y competencia del personal en temas de seguridad de la información.

Documentación del SGSI

La empresa debe mantener información documentada para asegurar la eficaz planificación, operación y control del SGSI.

Gestión de Documentos

Se deben establecer y mantener procedimientos para gestionar la creación, revisión y aprobación de documentos relacionados con el SGSI.

Control de Registros

La empresa AyA debe establecer y mantener procedimientos para la identificación, almacenamiento, protección, recuperación, retención y disposición de los registros del SGSI.

Gestión de Cambios

Deben existir procedimientos documentados para la gestión de cambios relacionados con el SGSI para asegurar la integridad del sistema.

Monitoreo y Medición del SGSI

Se debe planificar y documentar procesos para monitorear, medir y analizar regularmente el rendimiento del SGSI.

Auditorías Internas

La empresa debe establecer y mantener procedimientos documentados para realizar auditorías internas del SGSI.

Revisión por la Dirección del SGSI

Debe llevarse a cabo una revisión por la dirección del SGSI a intervalos planificados y documentar los resultados.

Acciones Correctivas y Preventivas

La empresa debe documentar procedimientos para la identificación y gestión de acciones correctivas y preventivas.

Desarrollo de una estrategia del Sistema de Gestión de Seguridad de la Información (SGSI) en la Empresa AyA bajo los lineamientos de la gerencia de proyectos

Para el desarrollo de la estrategia del Sistema de Gestión de Seguridad de la Información se definen las políticas de seguridad el alcance del SGSI para identificar y analizar los riesgos de amenazas y vulnerabilidades para seleccionar los controles y declarar la aplicabilidad garantizando su permanencia y cumplimiento por medio de auditorías.

Propósito

El propósito de la estrategia de un Sistema de Gestión de Seguridad de la Información es establecer las especificaciones técnicas de las políticas de Seguridad de la Información estableciendo límites desde los ámbitos de costos y tiempos.

Alcance

Identificar los requerimientos necesarios para garantizar el Sistema de Gestión de Seguridad de la Información para disminuir los eventos de seguridad en los diversos procesos de la empresa.

Aplicación

La estrategia de un Sistema de Gestión de Seguridad de la aplicación abarca todos los procesos de la compañía, en especial lo relacionados con la Dirección de TI en sus áreas de Infraestructura y desarrollo de software.

Política de Seguridad de la Información

La empresa AyA es consciente de la necesidad de diseñar una estrategia de un Sistema de Gestión de Seguridad de la Información para generar mayor confianza entre los clientes disminuyendo los riesgos de seguridad garantizando la confidencialidad, integridad y

disponibilidad de la información, cumpliendo la normatividad colombiana asegurando la mejora continua.

Objetivos de la Seguridad de la Información

Establecer las funciones y responsabilidades en la gestión de la Seguridad de la Información.

Garantizar el acceso a la información de manea segura y adecuada.

Fomentar la cultura de Seguridad de la información en el cliente interno y externo.

Identificar los riesgos relacionados con la perdida de información en el establecimiento de políticas de seguridad.

Roles y responsabilidades

La dirección de tecnología de la compañía establecerá los objetivos de Seguridad de la Información de acuerdo al área realizando seguimiento diario, semanal y mensual de las políticas establecidas garantizando el cumplimiento y la permanencia en el tiempo del Sistema de Gestión de Seguridad de la Información implementando ante los hallazgos acciones preventivas y correctivas actualizando el SGSI.

Identificación de riesgos de Seguridad de la Información

Los riesgos se identifican de acuerdo a las amenazas y vulnerabilidades estableciendo responsables de los riesgos en los activos de información partiendo de los procesos ejecutados por el personal de la empresa.

Tratamiento de riesgos

Al identificar un riesgo se validará si se implementa un control o sea realizan ajustes para su rechazo o aceptación analizando las ventajas y desventajas garantizando la Confiabilidad, Disponibilidad e Integridad de la información.

Evaluación del Sistema de Gestión de Seguridad de la Información

AyA se regirá por la norma de la ISO 27001 donde la evaluación de SGSI en primera medida se realizará de manera mensual por un lapso de 2 meses y al iniciar el proceso de maduración la evaluación se ejecutará mensualmente planteando mejoras a los 6 meses, y posterior seguimiento anual.

Auditoría interna

Se plantea realizar auditorías internas una vez al año ejecutada por personal diferente al equipo de implementación de las políticas de seguridad, quienes se capacitarán con la finalidad de lograr objetividad e imparcialidad, validando la continuidad de los controles de referencia del Anexo A de la ISO 27001, constituido por 11 controles agrupados en 14 secciones:

A.5: Políticas de Seguridad de la Información

A.6: Organización de la Seguridad de la información

A.7: Seguridad de los Recursos Humanos

A.8: Gestión de Recursos

A.9: Control de Acceso

A.10: Criptografía

A.11: Seguridad física y ambiental

A.12: Seguridad Operacional

A.13: Seguridad de las comunicaciones

A.14: Adquisición, desarrollo y mantenimiento de Sistemas

A.15: Relaciones con los proveedores

A.16: Gestión de Incidentes en Seguridad de la Información

A.17: Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio

A.18: Cumplimiento.

Políticas de seguridad de la información

Las políticas de seguridad de la información son presentadas por el alguacil de seguridad a la alta gerencia quien se encargará de mantener y actualizar el modelo cuya implementación estará regidas por la ISO 27001 estructuradas de la siguiente manera:

Título de la política

Definición

Vigencia

Fecha de actualización

Acciones de implementación

Responsables

Administración de la seguridad de la información

Incidentes de seguridad

Recolectores de eventos se instalarán en los servidores para monitorear eventos de seguridad y así definir las acciones de mejora plasmando la base de conocimientos.

Separación de ambientes

Se establecerán 3 ambientes donde 1 ambiente será exclusivo para el desarrollo de software, 1 ambiente de pruebas y 1 ambiente training.

Los 3 ambientes serán idénticos para garantizar que el paso a producción sea exitoso.

Al ambiente de pruebas sólo accederá el equipo de Aseguramiento de Calidad de Software (SQA) y al ambiente training es de uso exclusivo del área de implementación y clientes donde accederán como entorno de capacitación y/ esclarecer dudas en el funcionamiento del software.

Para homologar los ambientes el área de desarrollo indica las actualizaciones realizadas al área de SQA quien crea la batería de pruebas para ser ejecutada en el ambiente y certificar el paso a producción.

Control de código malicioso

Para controlar el ingreso de código malicioso a la red se prohibirá la descarga e instalación no autorizado y sólo el usuario administrador de red tendrá permiso para ejecutar las acciones.

Igualmente se planificará la ejecución de antivirus revisando diariamente las alertas generadas.

Al momento de presentarse algún evento de seguridad en el software en caso de requerirse alguna actualización se ejecutará sobre ambientes de pruebas para validar que no se generen problemas en el acceso a las aplicaciones.

Backup de la información

El respaldo de la información se realizará de manera diaria y un backup semanal ejecutando pruebas de restauración cada 2 meses para validar la calidad de la información.

En el procedimiento para resguardar la información se establecerá un procedimiento de rotulado de copias, el centro de almacenamiento debe contar con protección contra la humedad, altas temperaturas y demás aspectos ocasionados por condiciones ambientales.

Los medios físicos de almacenamiento se revisarán anualmente su estado para garantizar que no se presenten daños por deterioro, calidad o mejoras en la capacidad de almacenamiento.

Recolección de eventos

Se instalará software de auditoría para la recolección de eventos de seguridad consignando los intentos fallidos de ingreso a aplicativos y base de datos dando prioridad al intento de acceso a software no autorizado.

Gestión de vulnerabilidades

Al utilizar software licenciado se cuenta con actualizaciones constantes por parte del proveedor.

Igualmente se efectuará mensualmente el test de vulnerabilidades realizando el update o upgrade en los ambientes de desarrollo para garantizar la no afectación del servicio y posterior despliegue en ambiente de pruebas certificando la remediación de vulnerabilidades para desplegar en ambiente productivo.

Seguridad en las comunicaciones

Se estipulan políticas para la transferencia de información de manera segura garantizando su confidencialidad e integridad.

Control de redes

Se controlará el acceso a los sistemas de información de la empresa AyA utilizando credenciales seguras requiriendo su actualización mensualmente.

Seguridad en las redes

Solo se permitirá el uso de software autorizado, aquel que en un lapso de 2 meses no sea utilizado por el funcionario será desinstalado.

El acceso a los aplicativos será de acuerdo al perfil para evitar que los funcionarios visualicen información no autorizada visualizando sólo los módulos parametrizados por el administrador del sistema.

Separación de redes

Para garantizar la confidencialidad de la información se requiere la separación de redes para que los aplicativos se encuentren en diferentes segmentos de red para evitar afectaciones sobre toda la infraestructura tecnológica en cao de un ataque externo o en caso de requerir validar políticas en el firewall no se presente afectación en los ambientes de desarrollo, pruebas y producción simultáneamente.

Transferencia de Información

Se restringe el envío o recepción de información proveniente de terceros o cuentas de correo externas. Los correos cambian de com a .net donde las políticas no permiten la entrada o salida de correos diferentes al dominio de la empresa.

En caso de requerir información de un proveedor se habilitará una cuenta con permisos de envío y recepción de información custodiada por el oficial de Seguridad de la Información.

Con los proveedores se establecerán protocolos para la transmisión de información utilizando normas criptográficas para la codificación y la decodificación de los adjuntos para proteger la red de software y código malicioso.

Correo electrónico

Los funcionarios son responsables de la información proveniente de las cuentas donde la difusión de información que pueda vulnerarla confidencialidad de la compañía o permite el despliegue de correo malicioso acarrar sanciones disciplinarias.

Al sospechar de un mensaje malicioso no se debe abrir el correo evitando su replicación e informar inmediatamente al área de Seguridad de la Información.

Acuerdo de confidencialidad

Al vincularse a la empresa se debe firmar un acuerdo de confidencialidad donde no se podrá suministrar a terceros o compartir por medio de mensajería información de aplicativos, base de datos e infraestructura tecnológica.

Adquisición y desarrollo de software

Desarrollo seguro

Al momento de iniciar el diseño del software se establecer:

Responsables del diseño, aprobación y actualización del diseño seguro.

Documentación con las especificaciones técnicas a nivel de infraestructura y estructura de la base de datos y para identificar con facilidad posibles errores.

Las credenciales a utilizar durante el proceso de desarrollo deben ser resguardadas para proteger el código.

En las pruebas de funcionalidad se establecen los criterios de aceptación.

Ejecutar test de vulnerabilidades del código para encontrar posibles huecos de seguridad.

Establecer un sistema de versiones para controlar las actualizaciones indicando revisores, aprobadores, fecha de actualización y versión del documento.

Pruebas de seguridad

Para el desarrollo, adquisición o actualizaciones de software se establecerán pruebas de aceptación para validar la compatibilidad entre sistemas de información, integridad en relación a las comunicaciones, funcionalidad para conocer si el software cumple con lo estipulado en los diseños, desempeño para validar la eficiencia del sistema antes de realizar el despliegue en producción, pruebas de seguridad validando la autenticación, sesiones, intrusión, denegación del servicio y lógica del negocio.

Gestión de incidentes de seguridad

Reporte de eventos de seguridad

Es obligación de todos los colaboradores registrare y comunicar los incidentes de seguridad al oficial de seguridad de la información.

Evaluación de eventos de seguridad

Semestralmente se ejecutarán pruebas para medir la capacidad de respuesta ante los incidentes de seguridad para determinar la efectividad de prevención o solución del incidente.

Continuidad del negocio

Se plantea crear procedimientos para recuperarse rápidamente y el servicio del cliente interno y externo no se interrumpa ante fallas, desastres naturales, accidentes y/o ataques informáticos.

Continuidad de la seguridad de la información

Se capacitará a personal de las diversas áreas en cómo enfrentar las amenazas de seguridad de la información estableciendo mecanismos de divulgación y responsabilidades, implementando un plan de continuidad del negocio estableciendo cronograma bimensual de pruebas de recuperación de desastres.

Evaluación de continuidad del negocio

Se establecerán diversos escenarios analizando las posibilidades de recuperación del negocio.

Se realizarán pruebas de recuperación del negocio por medios de ambientes DRP los cuales se encuentran en diferentes zonas del país y ante un ataque deben levantar el servicio en el

menor tiempo posible sin generar interrupciones para el cliente teniendo en cuenta diversas tecnologías de software y hardware, y legislaciones de seguridad de la información.

Seguridad física

Se estipulan las políticas relacionadas con la infraestructura bajo responsabilidad del área administrativa cuya finalidad es el control de acceso de personal no autorizado.

Perímetro de seguridad física

Garantizar que las puertas de acceso estén protegidas mediante controles biométricos, alarmas y cerraduras protegidas a su vez de incendios, inundaciones, agentes ambientales, identificando las salidas de emergencia, dando prioridad a los elementos a proteger donde se almacene la información.

Control de acceso físico

Las áreas físicas se protegerán por medio de controles físicos llevando una bitácora de entradas y salidas permitiendo el acceso en momentos sólo de vital importancia donde la labor no se pueda ejecutar de manera remota, asignando tarjetas de control de acceso para los visitantes auditando el registro siendo escoltados por personal de las áreas involucradas recopilando la información en la oficina de control interno.

Control de acceso a zonas restringidas

Las instalaciones consideradas críticas se ubicarán en lugares donde no pueda acceder personal no autorizado ni tampoco de bastante flujo para garantizar la seguridad.

Los sitios de almacenamiento de información en especial DRP estarán en lugares discretos donde no sea fácil su ubicación por medio de señales en los pasillos.

En caso de existir ventanas sólo se abrirán internamente.

El control de acceso será con un acompañante del área no permitiendo el acceso de celulares o cámaras.

Protección de equipos

Los equipos se ubicarán en lugares donde no se presente acceso de personal no autorizado aislados de agentes contaminantes garantizando el aire acondicionado para mantener los equipos frescos en temperaturas donde no se afecte el procesamiento de información.

Seguridad de cableado

Proteger cableado eléctrico y de red de interceptaciones, interferencia o daños ambientales usando canales para su protección evitando su visibilidad en zonas públicas separando los cables de comunicaciones y eléctricos para solventar interferencias naturales afectando la transmisión de la información.

Seguridad de activos

Para el retiro de activos se controlará por medio de formatos de salida y entrada donde es primordial conocer la ubicación para garantizar la seguridad evitando el deterioro.

Escritorio limpio

La información en papel debe ser eliminada del puesto de trabajo y en caso de ser de vital importancia será guardada en unidades de almacenamiento para garantizar la seguridad de la información y a su vez evitar incendios ante la acumulación de papel.

Todos los escritorios tendrán llave asignada y deben permanecer cerrados y las llaves no estarán visibles siendo responsabilidad de cada colaborador.

Perfiles de acceso

Definición de activación e inactivación de perfiles de acceso dando permiso sobre ciertos módulos de los aplicativos según el perfilamiento garantizando la administración de perfiles garantizando la pronta inactivación en caso de detectarse violaciones de las políticas de seguridad de la información.

Mensualmente se inactivarán perfiles que sobrepasen 30 días sin acceder al sistema y para activación será justificada por el jefe inmediato.

Acceso de terceros a los aplicativos

En caso de requerir el ingreso a los aplicativos por parte de un tercero se realizará de manera controlada especificando hora de inicio y final para proceder a la activación e inactivación del acceso.

En caso de realizarse el acceso remoto la empresa AyA instalará la VPN estableciendo protocolos seguros en el equipo del tercero el cual debe cumplir con las políticas de seguridad brindando acceso por el tiempo determinado establecido para la actividad.

Monitoreo

Se instalará software de monitoreo de log para validar registros, alarmas, errores y bloqueos considerados eventos de seguridad al igual para medir el estado de servidores, performance y espaciado generando alertas cuando una partición esté ellgando al límite.

Separación de ambientes

Se homolgaran los ambientes de desarrollo, preubas y producción para garantizar que mejoras o fallos repliquen sin afectar funcionalidades. Igualmente se moverán a diferentes

segmentos de red para garantizar que al momento de aplicar políticas en firewall en etapa de desarrollo no impacte el ambiente productivo.

Claves de acceso

La contraseña es considerada personal e intransferible donde su propietario es el responsable de las acciones generadas con el usuario asignado.

Las contraseñas se cambiarán mensualmente sin permitir repetir las últimas siete contraseñas.

La contraseña será mínimo de 8 digitos incluyendo caracteres alfanuméricos, especiales, mayúsculas y minúsculas.

Copias de seguridad

La información alojada en los servidores se respaldará a diario, semanal y mensualmente. Al terminar el mes sólo se conservará la copia mensual custodiada en lugares protegigos de humo, agua y altas temperaturas.

Cada dos meses se realizará pruebas de restauración de la información para garantizar su confiabilidad, confidencialidad e integridad.

Cifrado de datos

Se implementarán métodos de cifrado de la información para garantizar la transmisión segura de datos cumpliendo con los acuerdos de confidencialidad considerando sensible cualquier tipo de información interna y externa.

Seguridad en Internet

Se limitará el acceso a páginas de entretenimiento y ocio, sitios de dudosa procedencia, cuentas de correo comerciales, redes sociales para controlar el ancho de banda.

En caso de requerir acceso auna página especializada debe contar con la previa autorización y solicitud del jefe directo para su evaluación ante el comité de seguridad de la información.

Conclusiones

Al realizar el análisis de las entrevistas se percibió la necesidad de implementar políticas de seguridad de la información a nivel de servidores, aplicativos y accesos lógicos y físicos, siendo conscientes que la empresa AyA debe brindar soluciones para una estrategia del Sistema de Gestión de Seguridad de la Información para contrarrestar las quejas del cliente externo donde el mismo cliente interno expone las debilidades pero hasta el momento no se ha brindado solución oportuna de los hallazgos e inconformidades siendo prescindible para los clientes al momento de la renovación de contratos donde ven necesario que la empresa adopte políticas por medio de un Sistema de Gestión de Seguridad de la Información.

Al ejecutar la encuesta se concluyó que el 77% de los colaboradores encuestados piensan y sienten que sólo la política de inactividad de sesiones de usuario se está utilizando parar proteger el acceso a las aplicaciones.

Referente a políticas de control de acceso físico a las oficinas se identificó que el ingreso y egreso a la empresa se realiza a cualquier hora y día, según lo indicó el 90%.

Sobre los controles de seguridad que se requieren implementar en la empresa se resalta el tecnológico con un 75%.

Referente al esfuerzo que cada colaborador debería hacer dentro de su rol para salvaguardar la seguridad de la información el 82% expresó no tiene conocimiento de cómo garantizar la confidencialidad, disponibilidad e integridad de la información.

Para determinar las posibles soluciones del diseño de la estategia del Sistema de Gestión de Seguridad de la Información se conocieron las características de los diversos sistemas de

seguridad de la información analizando los modelos OSSTMM 3, NIST, COBIT 5, ISO 27001 describiendo las características técnicas por medio de un cuadro comparativo.

Los resultados indicaron que referente a los sistemas de seguridad de información la calificación más alta es para el modelo propuesto por la ISO 27001 con 75 puntos siendo la opción más viable de acuerdo a la ponderación realizada por el director de tecnología

Se concluye que en el momento se requiere una estrategia del Sistema de Gestión de Seguridad de la Información en la empresa siendo de vital importancia para la gerencia y dirección de tecnología para tener productos y servicios de calidad y mejorar los procesos tecnológicos internos garantizando su ejecución de manera segura.

En general la importancia de contar una estrategia del Sistema de Gestión de Seguridad de la Información (SGSI) es fundamental en la era digital actual, donde la información es un activo valioso y crítico para el funcionamiento de las organizaciones. El SGSI ayuda a cumplir con normativas y requisitos legales relacionados con la seguridad de la información siendo crucial para evitar sanciones legales y mantener la confianza de clientes y partes involucradas.

La estrategia se definió al obtener un diagnóstico por medio de las entrevistas y encuestas donde se realizó un diagnóstico exhaustivo de riesgos presentes proponiendo procedimientos y políticas de seguridad para favorecer la mejora continua para revisar el desempeño y efectividad del Sistema de Gestión de Seguridad de la Información.

Recomendaciones

Es importante fortalecer los planteamientos de la gestión de proyectos al diseñar la estrategia del sistema de gestión de seguridad de la información bajo en la ISO 27001.

Se recomienda realizar revisiones periódicas del SGSI para asegurar de que sigue siendo relevante y efectivo actualizando la documentación, los procedimientos y las medidas de seguridad ejecutando auditorías internas a intervalos regulares para evaluar el cumplimiento de los controles y la efectividad del SGSI, utilizando los resultados de las auditorías para realizar mejoras continuas Utiliza la retroalimentación de incidentes, auditorías y revisiones para implementar mejoras constantes en el SGSI.

Igualmente es importante implementar un proceso formal de gestión de cambios para evaluar y gestionar cualquier cambio en la infraestructura, los procesos o las políticas que puedan afectar la seguridad de la información proporcionando formación y concienciación continua en seguridad de la información para garantizar que los empleados estén al tanto de las últimas amenazas y mejores prácticas de seguridad.

Se recomienda participa en comunidades y grupos de intercambio de información sobre seguridad para mantenerse actualizado de las tendencias y amenazas emergentes a través de la colaboración con otros profesionales de la seguridad.

Se recomienda asegurar que la alta dirección siga comprometida con el SGSI a lo largo del tiempo al ser la seguridad de la información una parte integral de la cultura organizacional.

De esta manera la empresa AyA estará mejor preparada para enfrentar los desafíos de seguridad de la información a lo largo del tiempo y adaptarse al entorno en constante evolución.

Bibliografía

Al-Karaki J.N., Gawanmeh A., El-Yassami S.(2022). GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking. Journal of King Saud University - Computer and Information Sciences 34(6), pp.3079-3095.

Anderson, M. (2007). Evaluating Information Assurance Products and Systems. CRC Press.

Antunes M., Maximiano M., Gomes R. (2022). A Client-Centered Information Security and Cybersecurity. Auditing FrameworkApplied Sciences (Switzerland) 12(9), 4102.

Auliani, A.S., Candiwan. (2021).Information Security Assessment on Court Tracking Information System: A Case Study from Mataram District Court 2021. IEEE 12th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2021 pp. 226-230.

Barbosa, F; Mancera, J. (2022). Informe de gestión 2022. Fiscalía General de la Nación.

Barrett, C., Dube, R., & Mody, R. (2012). Practical strategies for securing electronic health records. Journal of Healthcare Information Management, 26(2), 18-23.

Bicaku A., Zsilak M., Theiler P., Tauber M., Delsing J. (2022). Security Standard Compliance Verification in System of Systems. IEEE Systems Journal 16(2) pp.2195-2205.

Björnsdóttir S.H., Jensson P., de Boer R.J., Thorsteinsson S.E. (2022). The Importance of Risk Management: What is Missing in ISO Standards?.Risk Analysis 42(4), pp.659-691.

Brasoveanu R., Karabulut Y., Pashchenko I.(2022). Security Maturity Self-Assessment Framework for Software Development Lifecycle. ACM International Conference Proceeding Series 118.

Bygrave L.A.(2022). Security by Design: Aspirations and Realities in a Regulatory Context. Oslo Law Review 8(3) pp.126-177.

Camargo E.A.R., Pinzon M.A.R. (2022). The importance of information security in the public sector in Colombia. [La importancia de la seguridad de la información en el sector público en Colombia]RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao 2022(46) pp.87-99.

Caralli, R. (2012). The Costs and Benefits of Implementing the NIST Cybersecurity Framework. Software Engineering Institute.

Cirne A., Sousa P.R., Resende J.S., Antunes L. (2022). IoT security certifications: Challenges and potential approaches. Computers and Security 116, 102669.

Dwivedi, S., & Band, R. (2012). Empirical Evaluation of Open Source Tools for Security Testing. International Journal of Computer Applications, 51(20).

Garg, D., & Dohare, A. (2013). A comparative analysis of ISO/IEC 27001 and ISO/IEC 27005. International Journal of Advanced Research in Computer and Communication Engineering, 2(2).

Gray, D., Brown, S., & Macanufo, J. (2010). Gamestorming: A Playbook for Innovators, Rulebreakers, and Changemakers. O'Reilly Media.

Guggenmos F., Häckel B., Ollig P., Stahl B. (2022). Security First, Security by Design, or Security Pragmatism – Strategic Roles of IT. Security in Digitalization Projects Computers and Security 118, 102747.

Gutierrez Gutierrez, J. C., & Jimenez Villegas, H. C. (2024). Seguridad de la información, datos personales, habeas data dentro del ordenamiento jurídico colombiano 2020–2022. Repsoitorio Unilibre.

Herold, D. (2015). Applying COBIT 5 to Information Security. CRC Press.

Herold, D. (2015). Implementing ISO 27001 in a Windows Environment. CRC Press.

Imbaquingo, D.E., Herrera-Granda, E.P., Herrera-Granda, I.D., Guamán, V.L., Ortega-Bustamante, M.C. (2019). Evaluation of university informatic security systems: Teacher evaluation system a case study | [Evaluación de sistemas de seguridad informáticos universitarios caso de estudio: Sistema de evaluación docente]RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao 2019(E22), pp. 349-362.

Information Security Forum. (2018). Introduction to the Standard: ISO 27001. Information Security Forum.

International Organization for Standardization (ISO). (2013). Information technology - Security techniques - Information security management systems - Requirements (ISO 27001:2013). ISO.

ISACA. (2012). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. ISACA.

ISO/IEC. (2013). Information technology - Security techniques - Code of practice for information security controls (ISO/IEC 27002:2013). ISO.

Johansen J., Pedersen T., Fischer-Hübner S., Johansen C., Schneider G., Roosendaal A., Zwingelberg H., Sivesind A.J., Noll J.(2022). A multidisciplinary definition of privacy labelsInformation and Computer Security 30(3). University of Copenhagen, pp.452-469.

Kim, D., Lee, D., Kim, M., & Kim, J. (2008). A Practical and Complete Security Testing Methodology for Secure Software Development. In 2008 International Conference on Computational Science and Engineering. IEEE,Vol. 3, pp. 450-457.

Kotler, P., & Armstrong, G. (2018). Principles of Marketing. Pearson.

Litchfield, A., & Williams, J. (2015). An ISO 27001 case study - the implementation process. Information Security Journal: A Global Perspective, 24(2-3), 79-94.

Lykhova S., Servatiuk L., Shamsutdinov O., Sysoieva V., Hurina D. (2022). International and national standards on societal information security [Normas internacionales y nacionales sobre seguridad de la información en la sociedad]. Revista Cientifica General Jose Maria Cordova 20(38), pp.247-264.

Martelo, Raúl J.; Madera, Jhonny E.; Betín, Andrés D. (2021). Software for Document Management, a Modular Component of the Information Security Management System. ISMS, Vol. 26 Issue 2, p129-134. 6p.

Mateos Martín, C. (2021). Generación automática de Diagramas de Gantt. [Archivo digital UPM]. Sitio web: https://oa.upm.es/66279/.

Mell, P., & Scarfone, K. (2011). Common sense guide to cyber hygiene. National Institute of Standards and Technology (NIST).

Min, D., Kim, T. H., & Kim, H. (2012). Design of a security testing methodology for secure software development. International Journal of Software Engineering and its Applications, 6(2), 115-126.

Mogadem M.M., Li Y., Meheretie D.L. (2022). A survey on internet of energy security: related fields, challenges, threats and emerging technologies. Cluster Computing 25(4), pp.2449-2485.

Morelos-Gómez, J., Andrade-Quintero, E., & Ruiz-García, G. (2023). Evolución de la Gerencia de Proyectos de Construcción en la Aplicación del estándar PMI y las Metodologías Agiles. Revista científica anfibios, 6(1), 78-85.

National Institute of Standards and Technology (NIST). (2021). Computer Security Resource Center (CSRC). https://csrc.nist.gov.

OpenProject Community. (2020). OpenProject Documentation. Sitio web: https://docs.openproject.org/

Pallas Mega, G. (2019). Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. Repositorio Colibrí. Sitio Web: https://hdl.handle.net/20.500.12008/2954

Podrecca M., Culot G., Nassimbeni G., Sartor M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. Computers in Industry, 142, 103744.

Poma Ramos, A. (2021). SGSI con ISO 27001 aplicado a la empresa SOLTESI SAC del distrito de Jesús María 2021. Universidad César Vallejo. Sitio web: https://hdl.handle.net/20.500.12692/117149

Prowse, S. (2013). Information Security Governance Simplified: From the Boardroom to the Keyboard. CRC Press.

Razikin K., Soewito B. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. Egyptian Informatics Journal 23(3).pp.383-404.

Riascos Alomia, G. A., & Torres Montaño, A. F. (2022). Plan de gestión de seguridad de la información frente a las historias clínicas por la IPS Salud Max SAS. Repo

Rouse, M. (2019). NIST (National Institute of Standards and Technology). TechTarget. Sitio web: https://searchsecurity.techtarget.com/definition/NIST-National-Institute-of-Standards-and-Technology.

Safla Aranha, E. X. (2021). Propuesta de un sistema de gestión de seguridad de la información (sgsi) aplicado a la organización ABC. Universidad de las Américas. Sitio web: http://dspace.udla.edu.ec/handle/33000/13791

Samiei E., Habibi J. (2022). Toward a Comprehensive IT Management Methodology. IEEE Engineering Management Review 50(1), pp.168-185.

Scopel, F., & Pessôa, M. (2015). Security Testing Methodologies: A Comparative Study. In International Conference on Computer Safety, Reliability, and Security (pp. 106-118). Springer.

Taherdoost H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. Electronics (Switzerland) 11(14),2181. Sitio web: https://doi.org/10.3390/electronics11142181

Van Der Heyden, J. (2015). An introduction to ISO 27001:2013. Network Security, 2015(4), 9-13.

Van Grembergen, W., & De Haes, S. (2009). COBIT® 4.1, COBIT® 5, and Research: What's New? Information Systems Control Journal, 4.

Van Grembergen, W., & De Haes, S. (2013). COBIT 5 and IT governance—Understanding the basics. Information Systems Control Journal, 3.

Van Grembergen, W., & De Haes, S. (2013). COBIT 5 and IT governance—Understanding the basics. Information Systems Control Journal, 3.

Villegas-Ch, W., Ortiz-Garces, I., Sánchez-Viteri, S. (2021). Proposal for an implementation guide for a computer security incident response team on a university campus. Computers 2021, 10(8), 102. Sitio web: https://doi.org/10.3390/computers10080102

Yustanti, W., Qoiriah, A., Bisma, R., Prihanto, A. (2018). An analysis of Indonesia's information security index: A case study in a public university Open Access IOP. Conference Series: Materials Science and Engineering 296(1), 012038. Sitio web: https://iopscience.iop.org/article/10.1088/1757-899X/296/1/012038

Apéndices

Apéndice A

Entrevista al Director de Tecnología

Modelo de Gestión de proyectos para el Plan del Sistema de Seguridad de la Información en la empresa AyA

ENTREVISTA SEMIESTRUCTURADA

Entrevistado: Pablo Herrera
Cargo: Director de Tecnología

PREGUNTAS

¿Qué tipos de políticas de seguridad de la información se pueden seleccionar para solventar la problemática actual?
Sería importante diseñar un Sistema de Gestión de Seguridad de la Información para proteger la información de AyA. Las políticas debe implicar al personal, software, hardware, acceso lógicos y físicos, y almacenamiento.

¿La empresa puede brindar soluciones mediante un plan del Sistema de Gestión de Seguridad de la Información?
Si, la empresa puede garantizar soluciones con un SGSI para proteger todos los activos de la compañía. No sólo proteger los aplicativos de la compañía. Se debe proteger el acceso al edificio, oficinas y demás.

¿Se han presentado quejas de los clientes referente al riesgo de vulnerabilidad de la información al no contar con un Sistema de Gestión de Seguridad de la Información?
Si, los clientes han solicitado cuáles políticas de seguridad se están utilizando para evitar ataques informáticos al compartir parte de la infraestructura.

¿Se han presentado incidentes de seguridad de la información?
Si, se han presentado ataques informáticos dos de nuestros clientes externos en su propia infraestructura presentando indisponibilidad del servicio. Es de resaltar que internamente a la fecha no se han presentado ataques internos.

¿Tiene planeado realizar cambios en las políticas actuales para proteger la información de la empresa y clientes?
Si, en el momento se aplican políticas pero default de los aplicativos. No se cuenta con un diseño ni plan de Gestión de Seguridad Informática, siendo importante iniciar con el proceso para su planificación.

¿Cuál es el mayor problema presentado por no contar con un Sistema de Gestión de Seguridad de la Información?
El mayor problema es al momento de renovación de contratos con los clientes donde prácticamente nos solicita como requisito tener las certificación en ISO 27001y por ende disponer un Sistema de Gestión de Seguridad de la Información.

¿Cómo le gustaría que funcionara el Sistema de Gestión de Seguridad de la Información?
La forma de funcionar correctamente el Sistema de Gestión de Seguridad de la Información es donde no se afecten de manera negativa los actuales procesos de la empresa para evitar afectaciones a nivel de tiempo y costos.

Apéndice B

Entrevista al Jefe de Implementación

Modelo de Gestión de proyectos para el Plan del Sistema de Seguridad de la Información en la empresa AyA

ENTREVISTA SEMIESTRUCTURADA

Entrevistado: Dulfary Zapata
Cargo: Jefe de Implementación

PREGUNTAS

¿Qué tipos de políticas de seguridad de la información se pueden seleccionar para solventar la problemática actual?
Como jefe de implementación las políticas que se requieren implementar son la relacionadas con los aplicativos en los ambientes de desarrollo, producción y contingencia.

¿La empresa puede brindar soluciones mediante un plan del Sistema de Gestión de Seguridad de la Información?
Si, la empresa debe brindar las soluciones de carácter urgente para tener un Sistema de Gestión Informática para facilitar los procesos de capacitación.

¿Se han presentado quejas de los clientes referente al riesgo de vulnerabilidad de la información al no contar con un Sistema de Gestión de Seguridad de la Información?
Si, al momento de capacitar a los clientes en los aplicativos(software) indican porque no se perciben políticas de seguridad tan básicas como límite mínimo de caracteres y acceso con usuarios genéricos. De parte mía se explica al cliente que en el ambiente de desarrollo no se tienen aplicadas ciertas políticas a diferencia de los ambientes productivos.

¿Se han presentado incidentes de seguridad de la información?
Si, al momento de implementar no se despliega con políticas mínimas de seguridad de la información donde indica el cliente que se permite el acceso con el mismo usuario de manera simultánea.

¿Tiene planeado realizar cambios en las políticas actuales para proteger la información de la empresa y clientes?
Desde mi área no realizamos cambios en las políticas de seguridad de la información, peso si son necesarias para el cliente externo.

¿Cuál es el mayor problema presentado por no contar con un Sistema de Gestión de Seguridad de la Información?
El mayor problema es al momento de ofrecer y presentar el producto a los clientes donde lo primero que preguntan es por las políticas de seguridad de la información indicando que es un requisito para el proceso de contratación.

¿Cómo le gustaría que funcionara el Sistema de Gestión de Seguridad de la Información?
Me gustaría que todos los aplicativos y ambientes cuenten con cada una de las políticas establecidas en los Sistemas de Gestión de Seguridad de la Información para brindar tranquilidad a los clientes.

Apéndice C

Entrevista al Jefe de Infraestructura

Modelo de Gestión de proyectos para el Plan del Sistema de Seguridad de la Información en la empresa AyA

ENTREVISTA SEMIESTRUCTURADA

Entrevistado: Andrés Arévalo
Cargo: Jefe de Infraestructura

PREGUNTAS

¿Qué tipos de políticas de seguridad de la información se pueden seleccionar para solventar la problemática actual?
Desde el área de infraestructura se deben seleccionar políticas para servidores y acceso físico.

¿La empresa puede brindar soluciones mediante un plan del Sistema de Gestión de Seguridad de la Información?
Si, la empresa debe brindar las soluciones de seguridad de la información interna y externamente para reducir los riesgos a fallos de la infraestructura por un update o upgrade minimizando la posibilidad de ataques.

¿Se han presentado quejas de los clientes referente al riesgo de vulnerabilidad de la información al no contar con un Sistema de Gestión de Seguridad de la Información?
Si, al momento de presentarse alguna novedad en las transacciones los clientes indican que no se visualizan restricciones sobre las carpetas y cualquier usuario puede mover, copiar o eliminar la información.

¿Se han presentado incidentes de seguridad de la información?
Si, las particiones se han quedado sin espacio lo que ocasiona que los backup se ejecuten pero no se generen alertas al ser fallidos los procesos y en caso de restaurar la información afectaría su disponibilidad.

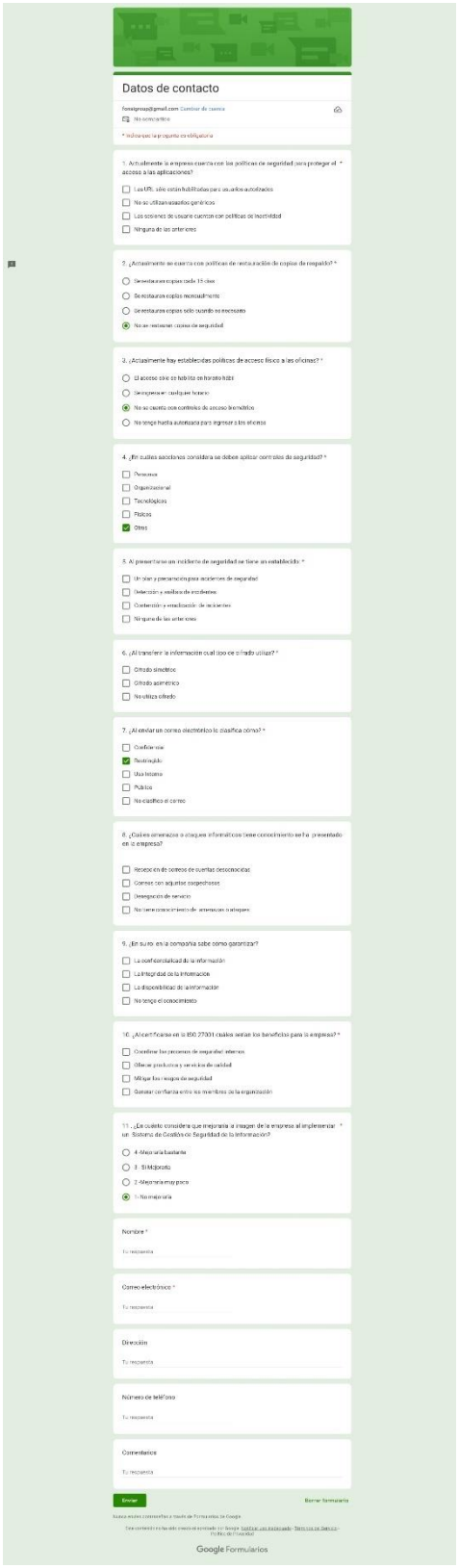
¿Tiene planeado realizar cambios en las políticas actuales para proteger la información de la empresa y clientes?
Se deben realizar cambios y hay unos requerimientos con el director de tecnología, para su aplicación deben ser primero aprobados y certificados en ambientes de pruebas para verificar que no se presente afectación en sistemas operativos o aplicaciones.

¿Cuál es el mayor problema presentado por no contar con un Sistema de Gestión de Seguridad de la Información?
Se ha presentado borrado de logs y al manejar el personal de soporte el super usuario es difícil conocer quien ocasionó la novedad.

¿Cómo le gustaría que funcionara el Sistema de Gestión de Seguridad de la Información?
Desde la infraestructura dar prioridad a las vulnerabilidades diseñando un plan de pruebas para garantizar siempre la disponibilidad del servicio.

Apéndice D

Encuesta a los colaboradores de la empresa AyA



Datos de contacto

fonsigroup@gmail.com Cambiar de cuenta

No comparte

* Indica que la pregunta es obligatoria

1. Actualmente la empresa cuenta con las políticas de seguridad para proteger el acceso a las aplicaciones? *

- Las URL´s/Ips están habilitadas para usuarios autorizados
- No se utilizan usuarios genéricos
- Los sistemas de usuario cuentan con políticas de inactividad
- Ninguna de las anteriores

2. ¿Actualmente se cuenta con políticas de restauración de copias de respaldo? *

- Se restauran copias cada 15 días
- Se restauran copias mensualmente
- Se restauran copias sólo cuando es necesario
- No se restauran copias de seguridad

3. ¿Actualmente hay establecidas políticas de acceso físico a las oficinas? *

- El acceso sólo se habilita en horario hábil
- Se ingresa en cualquier horario
- No se cuenta con controles de acceso biométrico
- No tengo hasta autenticarme para ingresar a las oficinas

4. ¿En cuáles secciones considera se deben aplicar controles de seguridad? *

- Personas
- Organizacional
- Tecnológicos
- Físicos
- Otros

5. Al presentarse un incidente de seguridad se tiene un establecido: *

- Un plan y precaución para acciones de seguridad
- Detección y análisis de incidentes
- Contención y erradicación de incidentes
- Ninguna de las anteriores

6. ¿Al transferir la información cual tipo de cifrado utiliza? *

- Cifrado simétrico
- Cifrado asimétrico
- No utiliza cifrado

7. ¿Al enviar un correo electrónico lo clasifica cómo? *

- Confidencial
- Restringido
- Uso interno
- Público
- No clasifico el correo

8. ¿Cuáles amenazas o ataques informáticos tiene conocimiento se ha presentado en la empresa?

- Respuesta de correos de cuentas desconocidas
- Correos con adjuntos sospechosos
- Desbalances de servicio
- No tiene conocimiento de amenazas cibernéticas

9. ¿En su rol en la compañía sabe cómo garantiza?

- La confidencialidad de la información
- La integridad de la información
- La disponibilidad de la información
- No tengo el conocimiento

10. ¿Al certificarse en la ISO 27001 cuáles serían los beneficios para la empresa? *

- Cumplimiento de requisitos internos
- Ofrecer productos y servicios de calidad
- Mitigar los riesgos de seguridad
- Ganar confianza entre los miembros de la organización

11. ¿De cuánto considera que mejoraría la imagen de la empresa al implementar un Sistema de Gestión de Seguridad de la Información? *

- 4- Mejoraría bastante
- 3- Si Mejoraría
- 2- Mejoraría muy poco
- 1- No mejoraría

Nombre *

Tu respuesta

Correo electrónico *

Tu respuesta

Dirección

Tu respuesta

Número de teléfono

Tu respuesta

Comentarios

Tu respuesta

Enviar

Borrar formulario

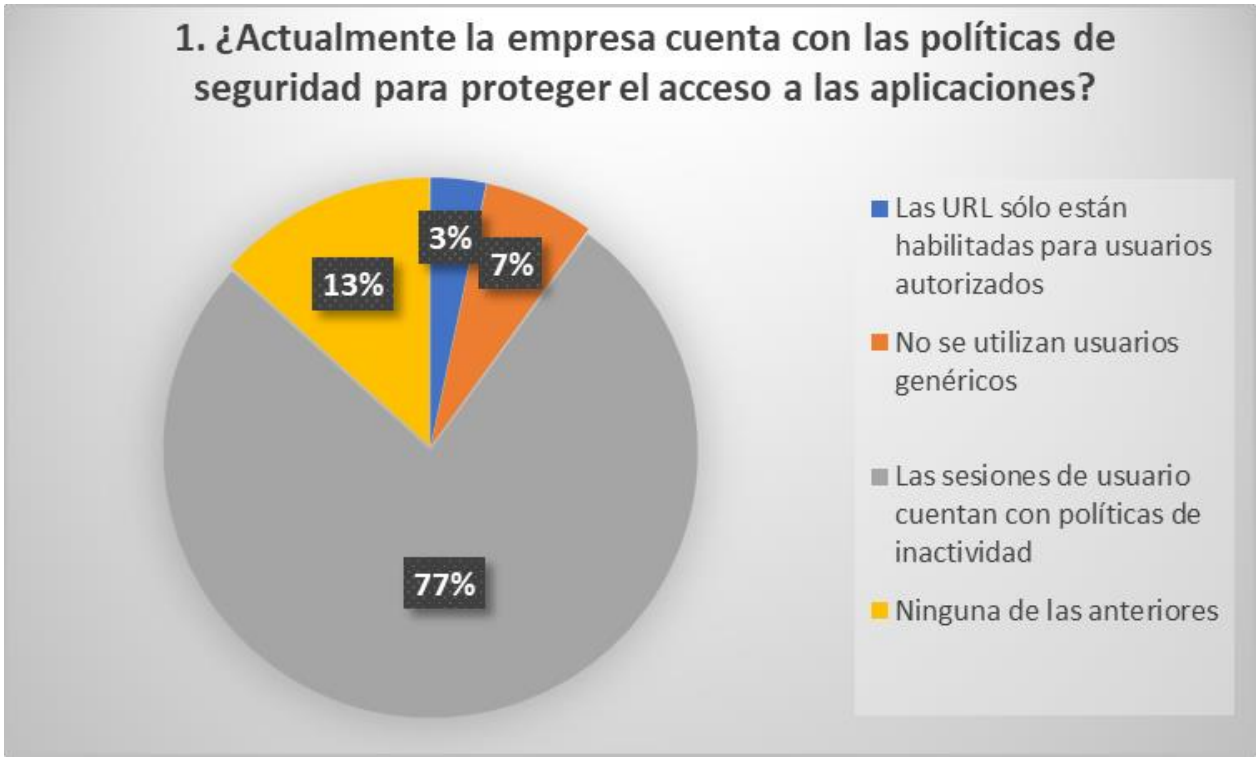
Nunca envíes contraseñas a través de Formularios de Google.

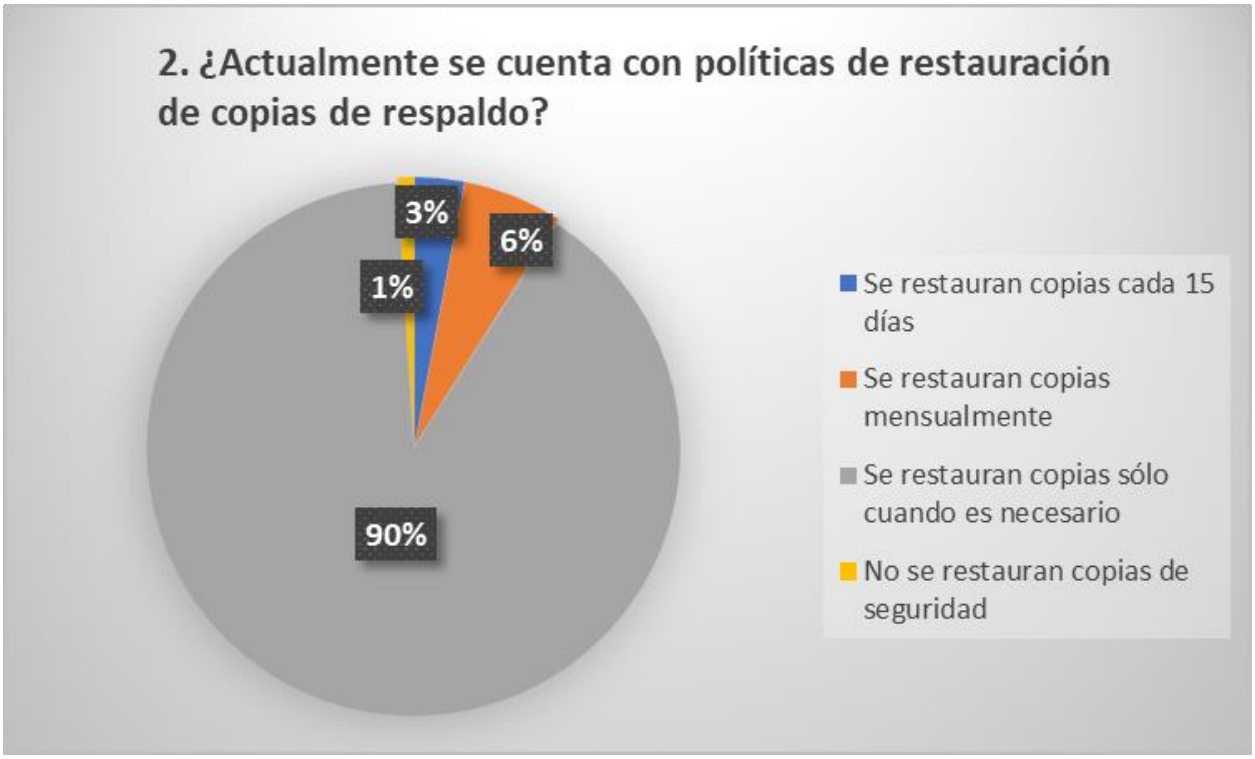
Este contenido no ha sido creado ni aprobado por Google. Notificar uso inadecuado - Términos del Servicio - Política de Privacidad

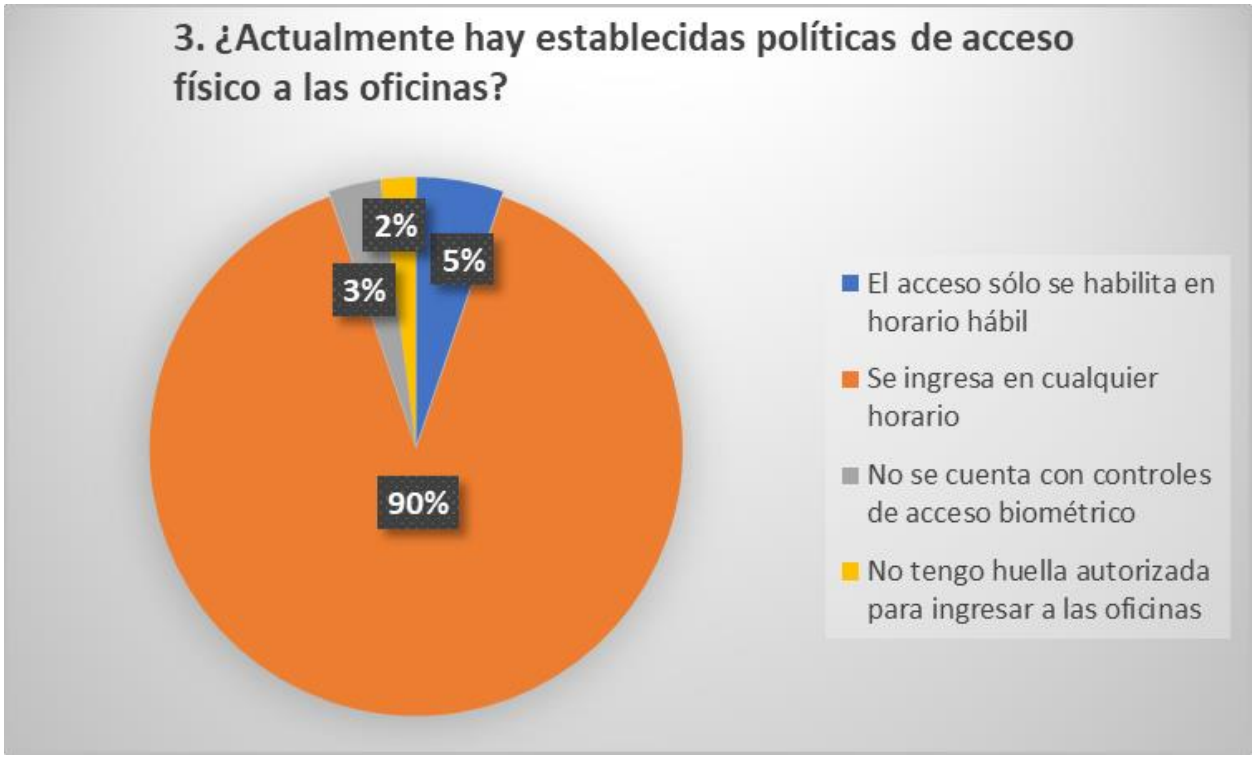
Google Formularios

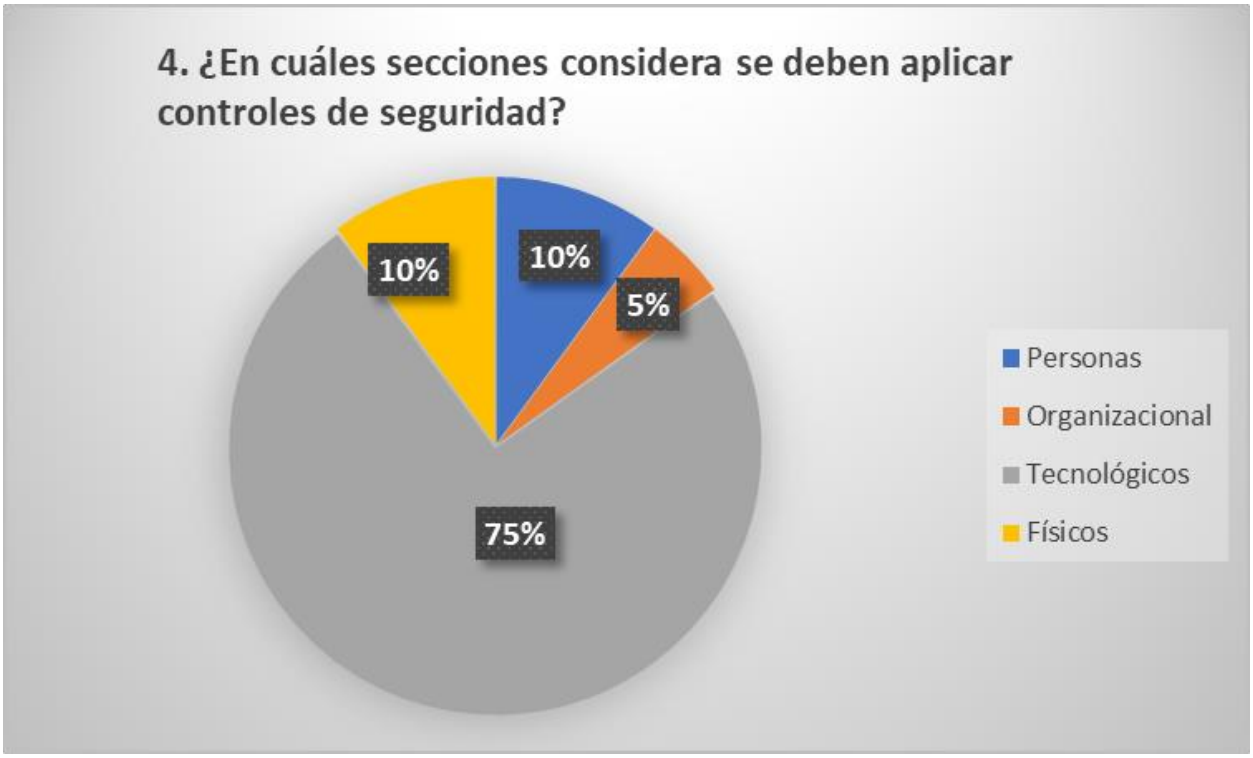
Apéndice E

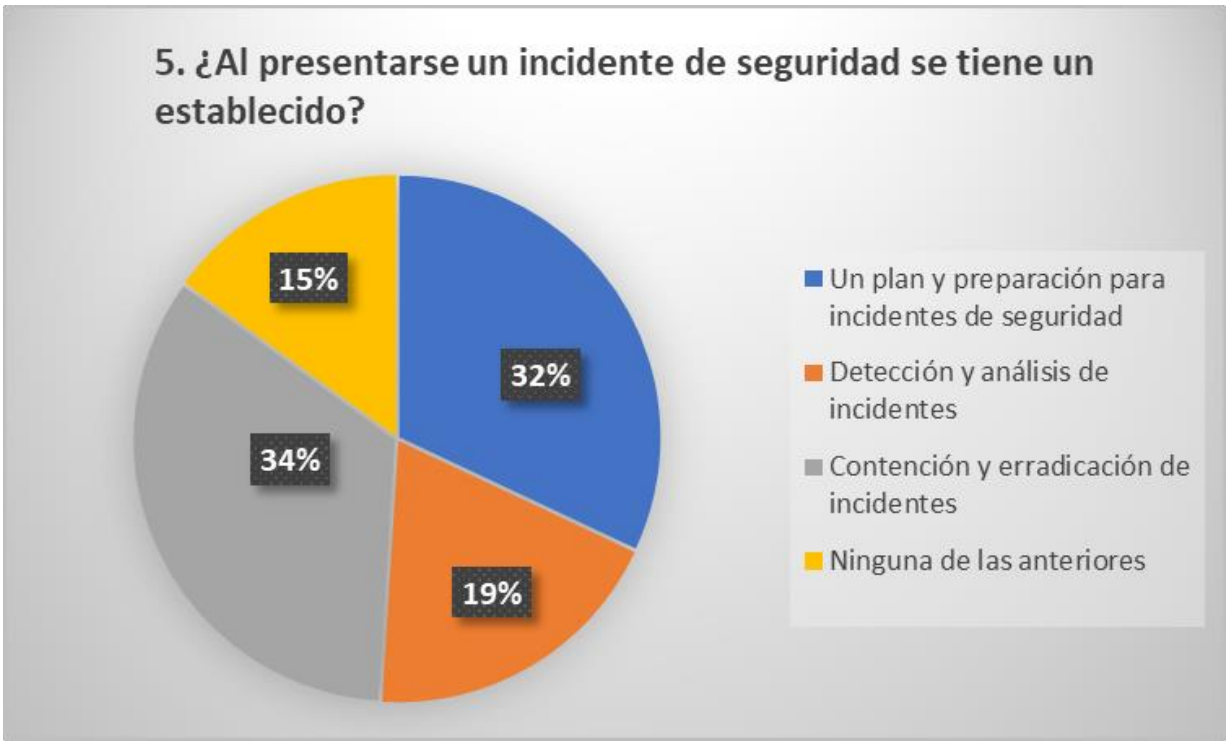
Tabulación de las encuestas realizadas a los colaboradores

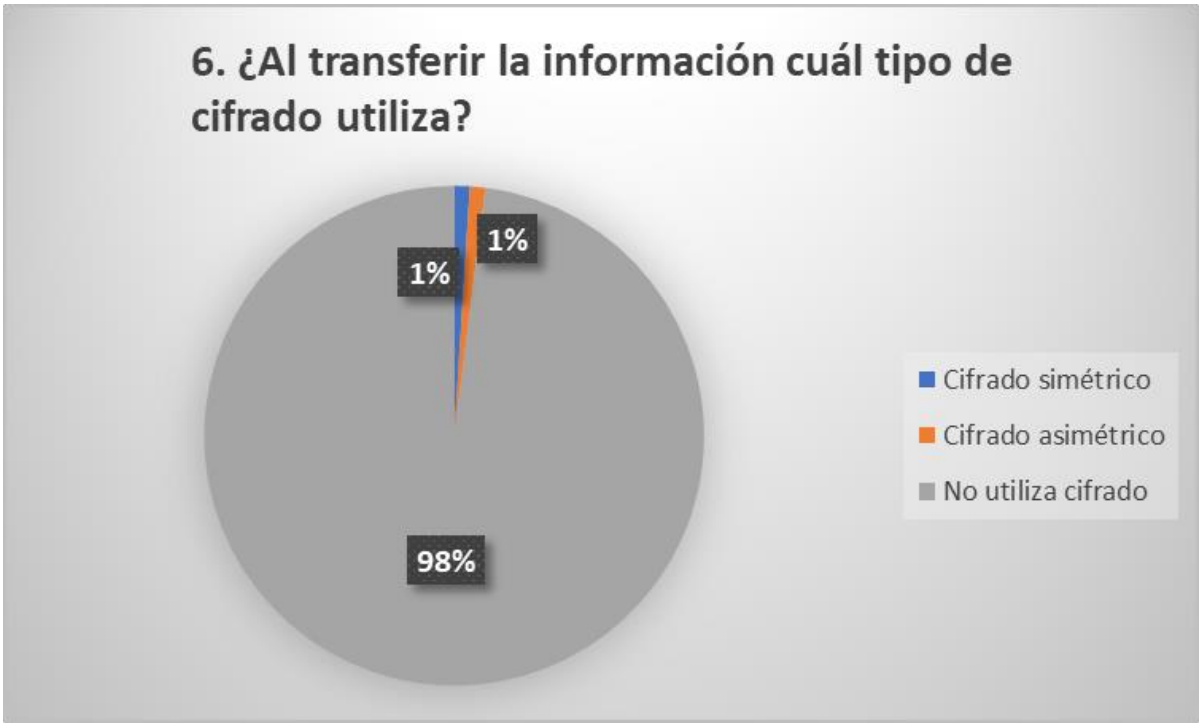


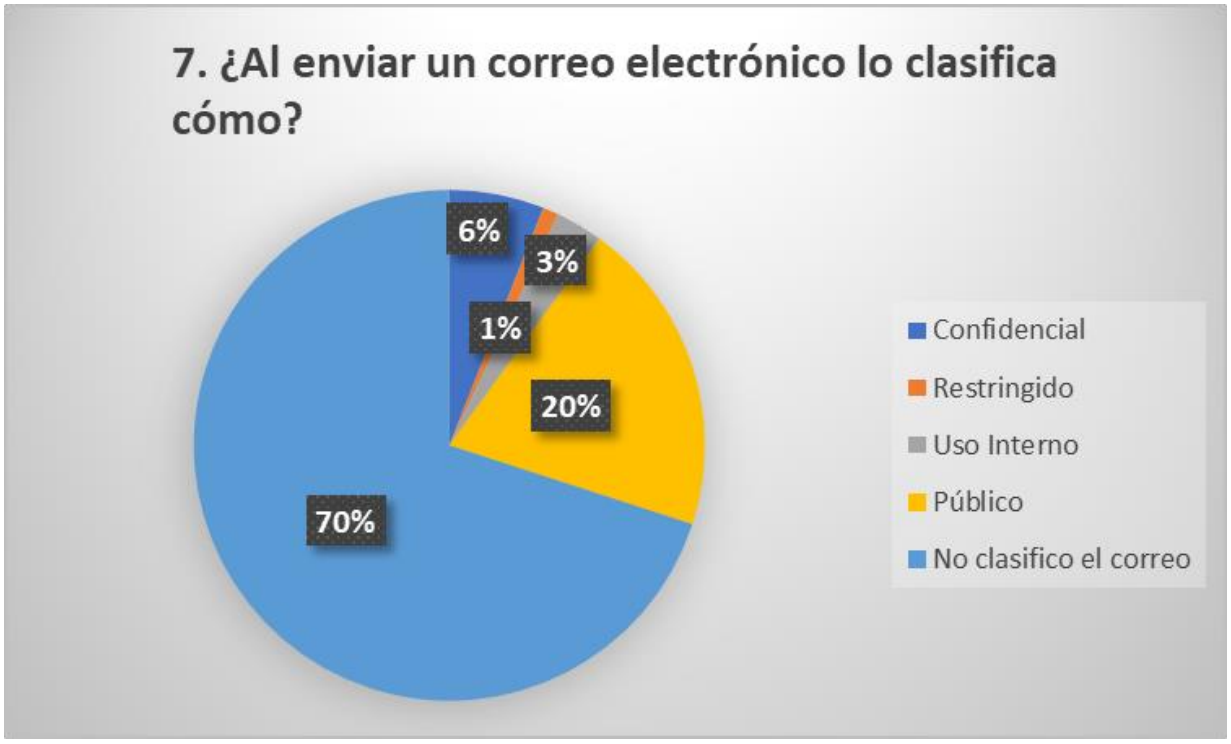


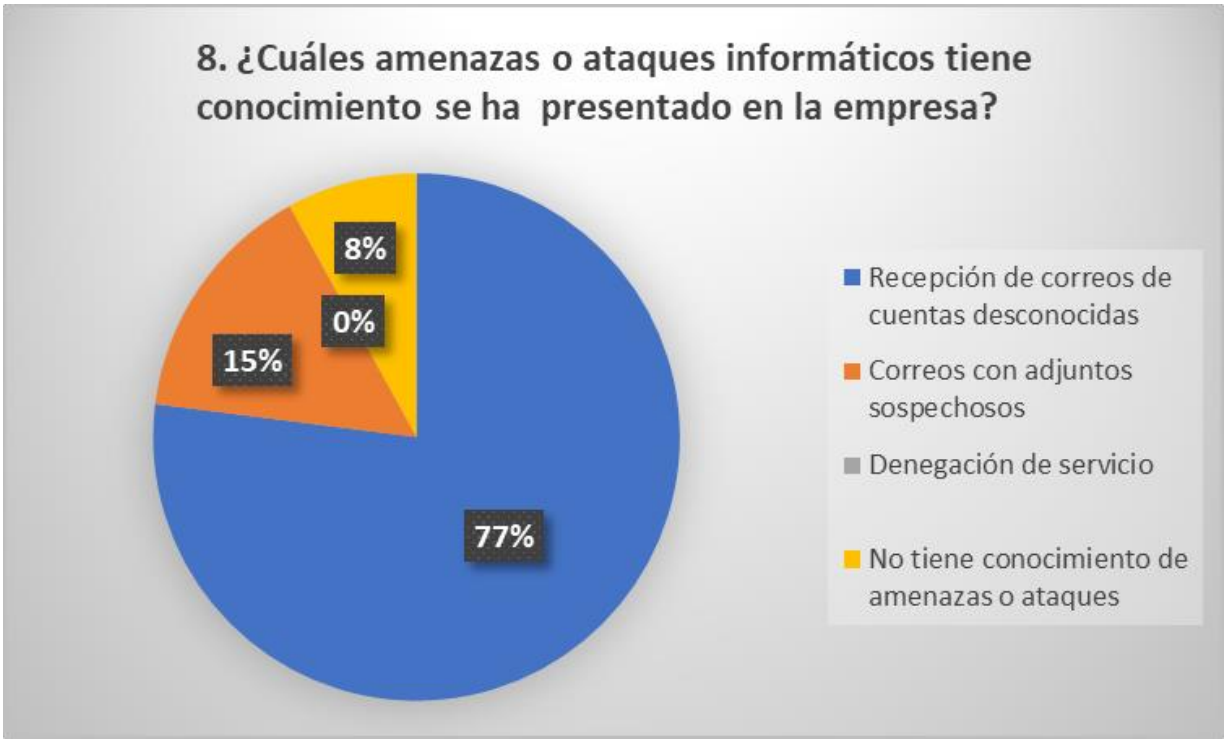

3. ¿Actualmente hay establecidas políticas de acceso físico a las oficinas?
2%
5%
3%
90%
El acceso sólo se habilita en horario hábil
Se ingresa en cualquier horario
No se cuenta con controles de acceso biométrico
No tengo huella autorizada para ingresar a las oficinas


4. ¿En cuáles secciones considera se deben aplicar controles de seguridad?
10%
10%
5%
75%
Personas
Organizacional
Tecnológicos
Físicos

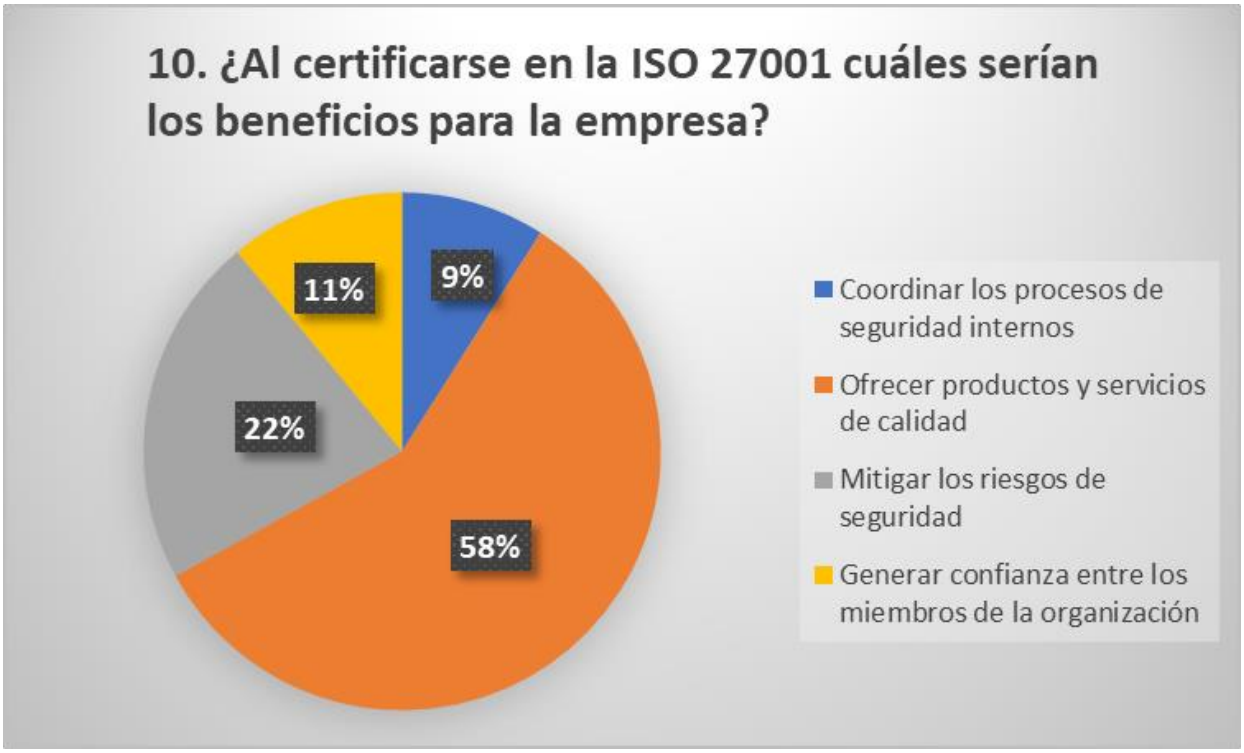

5. ¿Al presentarse un incidente de seguridad se tiene un establecido?
15%
32%
34%
19%
Un plan y preparación para incidentes de seguridad
Detección y análisis de incidentes
Contención y erradicación de incidentes
Ninguna de las anteriores

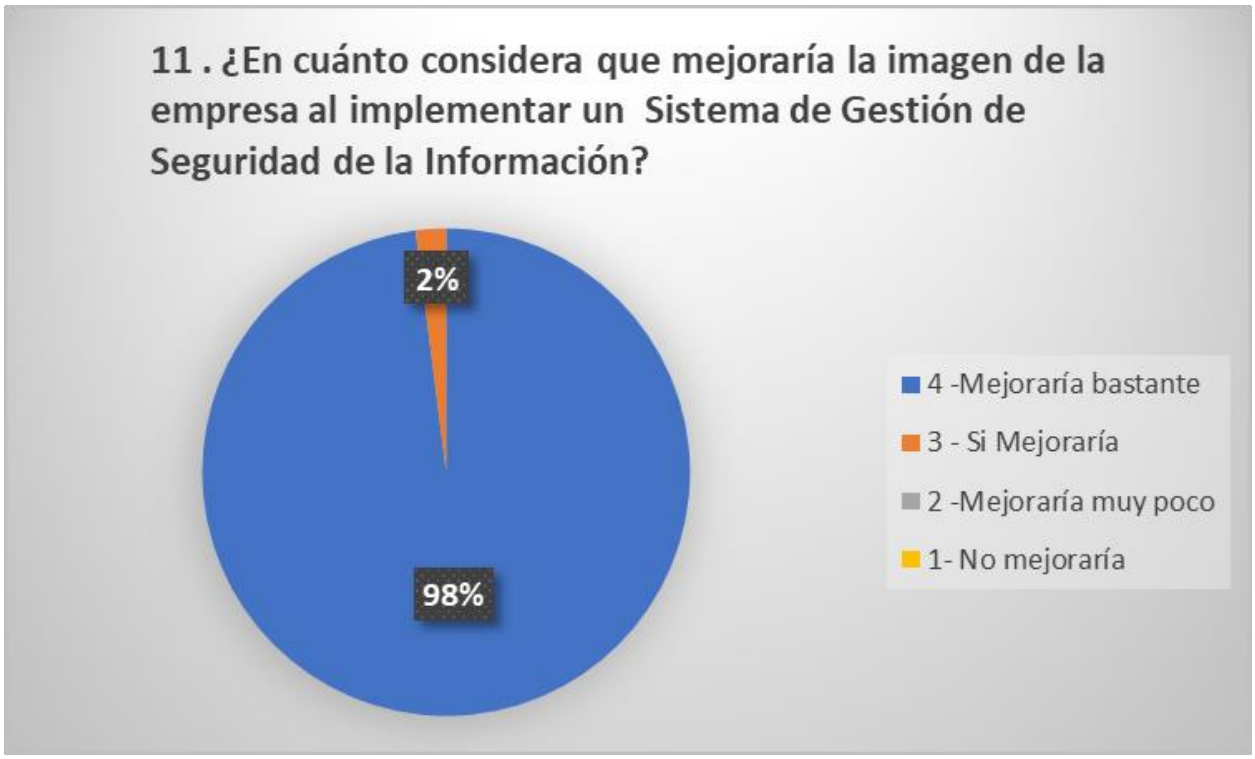

6. ¿Al transferir la información cuál tipo de cifrado utiliza?
1%
1%
98%
Cifrado simétrico
Cifrado asimétrico
No utiliza cifrado


7. ¿Al enviar un correo electrónico lo clasifica cómo?
6%
3%
1%
20%
70%
Confidencial
Restringido
Uso Interno
Público
No clasifico el correo


8. ¿Cuáles amenazas o ataques informáticos tiene conocimiento se ha presentado en la empresa?
8%
0%
15%
77%
Recepción de correos de cuentas desconocidas
Correos con adjuntos sospechosos
Denegación de servicio
No tiene conocimiento de amenazas o ataques


9. ¿En su rol en la compañía sabe cómo garantizar?
10%
1%
7%
82%
La confidencialidad de la información
La integridad de la información
La disponibilidad de la información
No tengo el conocimiento


10. ¿Al certificarse en la ISO 27001 cuáles serían los beneficios para la empresa?
9%
58%
22%
11%
Coordinar los procesos de seguridad internos
Ofrecer productos y servicios de calidad
Mitigar los riesgos de seguridad
Generar confianza entre los miembros de la organización


11 . ¿En cuánto considera que mejoraría la imagen de la empresa al implementar un Sistema de Gestión de Seguridad de la Información?
2%
98%
4 -Mejoraría bastante
3 - Si Mejoraría
2 -Mejoraría muy poco
1- No mejoraría