Diseño de un sistema de Gestión de seguridad de la información (SGSI) para la asociación ARFUSOG, recolectora de residuos sólidos de la ciudad de Sogamoso, mediante el uso de herramientas de gestión de proyectos

María Eugenia Verona Pérez

Vanessa Ventura Ríos

Asesor

Edward Fernando Toro Perea

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas Tecnología e Ingeniería ECBTI

Maestría en Gerencia de Proyectos

2022

Dedicatoria

Dedico esta tesis a Dios por permitirme adquirir nuevos conocimientos y poder alcanzar una meta más en mi vida. A mi esposo Carlos Augusto Espinosa e hijos Keidy Andrea y Kevin Alejandro, por apoyarme de manera incondicional en el proceso y ser el pilar fundamental para lograr mis sueños.

Por ende, dedico el trabajo primeramente a Dios, porque en su infinita misericordia me permitió adquirir el conocimiento necesario para culminar esta tesis; a mis padres y a Nevis Alfredo cubillos por apoyo incondicional en el proyecto tan importante para mí.

A los docentes de la Maestría en Gerencia de proyectos, que fueron promotores y motivadores del proceso de formación, gracias por entregarnos parte de su conocimiento.

Al doctor Edward Fernando Toro, le expresamos nuestro agradecimiento por su invaluable asesoría en el trabajo de grado y por ayudarnos a enfocar la investigación de manera clara en cada una de las etapas del proyecto y, por su paciencia y por exigirnos excelencia como profesionales durante el desarrollo de esta tesis.

Agradecimientos

Gratitud infinita a Dios y a mi familia, que se involucraron en mi proceso de formación para ayudarme a lograr las metas propuestas. A la Universidad y a todos los docentes que compartieron su conocimiento con nosotras para formar profesionales de calidad e integridad.

En primer lugar, agradezco a mi director/a de tesis, el doctor Edward Fernando, por su dedicación y compromiso hacia mi proyecto, así como su pasión por la investigación, fueron una fuente constante de inspiración para mí. Gracias a usted, pudimos desarrollar un trabajo de grado que estoy segura será de gran valor para mi carrera profesional.

Agradezco a ARFUSOG, por proporcionarme la información necesaria para llevar a cabo la investigación.

Por último, quiero agradecer a Dios por su amor y por darme la fuerza y la perseverancia para terminar este proyecto. Espero que este trabajo sea útil para futuras investigaciones y que pueda contribuir de alguna manera al desarrollo de mi campo de estudio.

Resumen

ARFUSOG, es una asociación relativamente nueva que fue creada en el año 2017, con la finalidad de recolectar residuos sólidos no aprovechables mediante el uso de tres macro rutas y 16 micro rutas ya identificadas, cabe mencionar la inexistencia de un sistema de seguridad de la información que especifique los requisitos necesarios para establecer, implantar, mantener y mejorar el SGSI, siendo éste un enfoque de mejora continua que conlleva a los procesos de planear, hacer, verificar y actuar.

Esta propuesta de investigación tiene como finalidad diseñar un sistema de Gestión de seguridad de la información (SGSI) para la asociación ARFUSOG. La metodología para el diseño del Sistema SGSI, se basará en la utilización de herramientas de gestión de proyectos Matriz DOFA y el Diagrama de Pareto, ya que son técnicas que facilitan la identificación de los problemas que se presentan en la organización, restricciones y la forma de resolverlos.

De la misma manera se establecerán las personas responsables de salvaguardar la información, los cuales deben definir el alcance y los procesos críticos a proteger, la política de seguridad de la información, los recursos necesarios para operar, las mejoras en el mantenimiento, los procedimientos destinados a garantizar la confidencialidad de la información y la minimización de riesgos.

Palabras clave: Diseño, Sistema, SGSI, Gestión, Herramientas, Proyecto

Abstract

ARFUSOG, is a relatively new association that was created in 2017, with the purpose of collecting unusable solid waste through the use of three macro routes and 16 micro routes already identified, this company is located in the department of Boyacá , Sogamoso municipality, which has a population close to 115,000 inhabitants; the entity has been implementing operational and administrative actions in accordance with current legal regulations, especially Decree 596 of 2016; In accordance with the above, the company does not have an information security system that specifies the necessary requirements to establish, implement, maintain and improve an Information Security Management System, this being an improvement approach. continuum that leads to the processes of Plan, Do, Control and Act.

The lack of a clear and defined information system inevitably facilitates unauthorized access by third parties to the information network and the equipment that is connected to it and consequently the theft of confidential company information. Therefore, this research proposal aims to design an Information Security Management System (ISMS) for the ARFUSOG association.

The methodology for the design of the SGSI System will be based on the use of project management tools SWOT Matrix and the Pareto Diagram, since they are techniques that facilitate the identification of problems that arise in the organization, restrictions, and the form to solve them. In the same way, those responsible for security, scope, and critical processes to protect, information security policies, necessary resources for the operation, maintenance improvement, through these procedures are intended to ensure the confidentiality of the information and minimize the risks.

***Keywords*:** Design, System, SGSI, Management, Tools, Project

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

La gestión de proyectos contiene una serie de aspectos positivos para las diferentes áreas de la organización porque hace uso de metodologías, herramientas y procesos que permiten Planificar, hacer, verificar y actuar (ciclo PHVA); un ejemplo claro es la propuesta que se avenido desarrollando en la Maestría en Gerencia de proyectos titulada **"**Diseño de un sistema de Gestión de seguridad de la información (SGSI) para ARFUSOG, empresa recolectora de residuos sólidos de la ciudad de Sogamoso, mediante el uso de herramientas de gestión de proyectos". El sistema se basará en la norma ISO-27001 en su literal 2. (a) comprender los requisitos y la política de seguridad de la información.

Es oportuno mencionar en este punto que, este proyecto de investigación parte inicialmente de la formulación planteamiento de problema en el cual se sintetiza las falencias, necesidades o dificultades a cerca del sistema de información al interior de la asociación ARFUSOG, posteriormente se formulan los objetivos en rutados al diseño un sistema de estrategias de seguridad de la información, para la determinación de plan de mejoramiento en gestión de la seguridad de la información, en efecto quedan plasmados antecedentes teóricos, investigaciones previas y leyes como sustento del presente proyecto, a su vez que la metodología a la cual se acoge el proyecto es mixta con procedimientos metodológicos como horizonte de la propuesta, compuesto por 3 fases que contienen 6 etapas y 20 tareas donde se pretende obtener la información directa de la asociación, analizar resultados de las encuestas, entrevistas y diagnósticos, además analizar debilidades del sistema a través de las herramientas de gestión de proyectos, estimación posibles soluciones del SGSI, por consiguiente se estiman conclusiones como resumen final de los procesos descritos y recomendaciones relacionadas de tal manera que se preserve la confidencialidad, disponibilidad y la integridad de la información.

Planteamiento del Problema

Sogamoso es una ciudad colombiana situada en el centro-oriente del departamento de Boyacá, a 210KM al noroeste de Bogotá, actualmente cuenta con 114.676 habitantes, el cual representa el 9.02% del total de la población del Departamento.

A por ende el propósito de la asociación de recicladores por el futuro de Sogamoso (ARFUSOG), lidera un proyecto macro para la optimización de los puntos de recolección de residuos sólidos aprovechables en la Macro ruta – Centro en la ciudad, tomando en consideración el decreto 596 de 2016. El problema que se presenta en la empresa es la falta de un sistema de Gestión Seguridad de la información que le permita a la entidad una adecuada gestión del riesgo de la información, activos de información identificados y roles y funciones asignadas a cada empleado.

En efecto, el hecho de que la asociación ARFUSOG no cuente con sistema de estrategias planeadas de seguridad de la información mediado por herramientas de gestión de proyectos, puede deberse al desconocimiento del sistema de seguridad de la información, falta seguimiento y compromiso de la alta dirección, ausencia de documentación e información estandarizada, inexistencia en la definición de roles y responsabilidades, inseguridades en la adecuada gestión de activos de información y por sus puesto desconocimiento de los riesgos y amenazas que estos pueden causar a la empresa; por consiguiente podría mostrarse como una resistencia al cambio de los procesos, entre otros aspectos relevantes, que en mayor o menor medida impactan significativamente en la asociación y se convierten en un llamado para generar estrategias conscientes para el mejoramiento de la seguridad de la información.

Las deficiencias en el manejo de la documentación e información estandarizada podrían afectar notablemente el seguimiento y calidad en procesos de estandarización. (Russell, 2013).

No obstante, dicha propuesta de recolección de residuos sólidos de ARFUSOG, no cuenta con un sistema de estrategias de seguridad de la información (SGSI), que se apoye en herramientas de gestión de proyectos.

Según, Baldecchi (2014) “se garantiza la seguridad de la información (SI) mediante una estructura de buenas prácticas, definidas gestión de riesgos, políticas, procesos, procedimientos, controles, revisiones y mejoras” (p.6).

De modo que resulta prudente mencionar que las herramientas de gestión de proyectos funcionan como elemento diferenciador que busca precisamente ser un apoyo para que asociación ARFUSOG organice, planifique, documente, y gestione mejor sus procesos, con la ayuda de herramientas como matriz DOFA, espina de pescado, diagrama de Pareto, lluvia de ideas, entre otros instrumentos. Cabe entonces señalar que Wallace (2014) afirma que “la gestión de proyectos debe considerarse como una herramienta para gestionar cambios únicos, los cambios implicados se planifican e implementan mejor utilizando técnicas y herramientas de gestión de proyectos” (pp. 12-42).

Pregunta de Investigación

¿Cómo garantizará el uso de herramientas de gestión de proyectos y el diseño del SGSI la integridad y confidencialidad de la información de la empresa ARFUSOG?

Justificación

La justificación principal se centra en el diseño del Sistema de Gestión de Seguridad de la Información (SGSI) propuesto en la Asociación de Residuos Sólidos Reutilizables de Sogamoso (ARFUSOG), de acuerdo con las buenas prácticas propuestas por la norma técnica ISO/IEC. 27001, con el fin de garantizar el aseguramiento de la información en línea con la filosofía misionera de la empresa, el sistema SGSI se convierte de esta forma en una herramienta estratégica que minimiza el riesgo de la operación de los activos de información y garantiza la adecuada gestión administrativa y financiera de la organización.

La inexistencia de un SGSI en ARFUSOG, favorece la inseguridad de la información, debido a los múltiples riesgos y amenazas derivados de los cambios continuos y dinámicos que constituyen el desarrollo de las tecnologías de la información, es necesario que las organizaciones desarrollen una estrategia de seguridad basada en la identificación de riesgos que este alineado con las necesidades del negocio, el objetivo es contar con un modelo de seguridad de la información que soporte y apalanque los objetivos estratégicos de la organización.

El diseño del SGSI demuestra compromiso por parte de la organización e impulsa a la empresa a cuantificar, evaluar y realizar correcciones pertinentes al proceso en cuanto a la información que se debe resguardar, de la misma manera genera confianza a los socios del proyecto, debido a que está compuesto por una estructura que define roles y funciones de los colaboradores regidos por políticas y procedimientos implementados para la gestión de activos y más información del proyecto, fomentando una cultura de seguridad en todos los niveles del proyecto buscando la mejora continua del proceso.

A través del sistema SGSI, la entidad promoverá con sus colaboradores los procedimientos para que el proyecto pueda identificar amenazas que afecten la disponibilidad de

la información de tal manera que le permita establecer actividades y equipo para disminuir los efectos negativos en caso de pérdida de la información.

Un SGSI ayudará a la entidad a tener un enfoque de gestión de riesgos para medir y clasificar aquellas posibles violaciones a los sistemas de información, de manera que podrá evaluar los controles establecidos a través de indicadores de gestión, y así mismo, podrá dar una respuesta oportuna y rápida.

La seguridad informática se realiza para proteger los datos existentes y futuros de una organización, de esta manera se da seguimiento a las políticas de seguridad definidas para evitar problemas futuros y minimizar el riesgo. Las Políticas de seguridad informática se convierten en una herramienta de control y proteger de la información para la empresa.

Objetivos

Objetivo General

Diseñar un sistema de estrategias de seguridad de la información de una empresa recolectora de residuos; para la determinación de plan de mejoramiento en Gestión de la seguridad de la información (SGSI) de la asociación ARFUSOG de la ciudad de Sogamoso.

Objetivos Específicos

Determinar las características del sistema de Gestión de Seguridad de la información de la empresa Asociación ARFUSOG, con la finalidad de establecer un diagnóstico del SGSI.

Analizar el diagnóstico del sistema de Gestión de seguridad de la información, con el fin de determinar las posibles soluciones del SGSI.

Evaluar las posibles soluciones del sistema de Gestión de seguridad de la información, para la determinación del plan de mejoramiento del SGSI, de la empresa asociación ARFUSOG.

Marco Referencial

Marco Conceptual

El plan inicial del desarrollo de un marco teórico que sustente la investigación a realizar incluye no sólo los supuestos teóricos de los que parte el investigador, sino también conforma la manera en la que el investigador recoge sus datos, que a su vez determina o establece los límites de las clases de análisis que pueden emplearse. (Reidl &Martínez, 2012, p147).

ISO-27001

Señala que "es la norma internacional para los sistemas de gestión de la seguridad de la información (SGSI). Proporciona un marco robusto para proteger la información que se puede adaptar a organizaciones de todo tipo y tamaño. (NQA, 2013, p.4).

SGS

Es el diseño, implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad. (FIRMA-e.com, 2013,p.1).

Sistema de información

Cuando se habla de un sistema de información (SI) se refiere a un conjunto ordenado de mecanismos que tienen como fin la administración de datos y de información, de manera que puedan ser recuperados y procesados fácil y rápidamente. (Editorial Etecé, 2023,p.1)

Ciclo PHVA

El ciclo PHVA (Planificar-Hacer-Verificar-Actuar) es una estrategia interactiva de resolución de problemas para mejorar procesos e implementar cambios. Al seguir el ciclo PHVA los equipos desarrollan hipótesis, ponen a prueba las ideas y las mejoran. (Martins, 2022, p.1)

Registros

Los registros pueden considerarse como un instrumeto indispensable por la ayuda que ofrece a quien estan en busca de información respecto a situación, acontecimiento, fenomeno entre otros, e incluso puede servir de sorporte. Afirma Carrillo (2016), "el ciclo texto contexto se desarrolla en un determinado registro, que se acomoda comunicativamente a la situación dentro de la complejidad y variabilidad del uso de la lengua" (p.1).

Desde luego, es casi imposible separar los registros de la lingüística, por tanto, Carrillo (2016) menciona que "el registro condiciona los niveles lingüísticos de vocabulario y sintaxis" (p.7). en complemento, según (Tarry, 1995 citado en Carrillo, 2016, p.7)" el registro privilegia el contexto de la situación sobre el contexto social más amplio"

Encuesta

La encuesta ha ido tomando relevancia a medida que transcurren los años, sin embargo esta tecnica ha tomado posesión en terminos de investigación estanadirzadas que suelen ser, además porque con su aplicación se abarca de forma extenza a la población a la cual se dirrige el estudio. Por esta razon menciona, Caballero (2017) "La elaboración de encuestas ha jugado un papel fundamental en la intención de conocer las apreciaciones que tienen las personas frente a un tema determinado" (p.9). Más que ser técnica que nutre una investigación de datos importantes, cumple una función integral y detallada, de la misma manera hace referencia a que las personas, son, hacen, piensan, opinan, sienten, esperan, desean, quieren u odian, aprueban o desaprueban, o los motivos de sus actos, opiniones y actitudes" (Hernández et. al, 2009, p.4 citado en Caballero, 2017, p.10).

Matriz DOFA

La matriz DOFA como herramienta de gestión de proyectos es muy utilizada en terminos empresariales precisamente pára detección y conocimiento de las debilidades, oportunidades, fortalezas y amenazas, que permitirá a los directivos de la empresa tener consciencia de los obstulos para la organización, analizar con que cuenta la empresa para enrutarse nuevamente a los objetivos previamente proyectados, disminuir factores negativos y potencializar los postivos entendiendo que es metodo con visión estrategica. Considerablemente la DOFA es un apoyo al proceso de planificación, es de uso sencillo sin perder su carácter analitico, y por supuesto se trabaja con los directivos de la empresa. Entorno a las ventajas internas se encuentra, conocmientos de los puntos debiles y amenzantes, el proceder de la empresa, construcción de estrategias con base a un diagnostico previo, asu vez realaciona la inversion y la rentabilidad. Sin refirier a aspectos externos en cuanto a ventajas, conocimiento de proveedores, clientes, mercados, competidores directos y no directos, mercados, bancos, el habitad y el impacto de la empresa, entre otros asuntos. (García, 2019, pp. 1- 47).

La acogida que ha tenido el instrumento DOFA, en las organizaciones se debe a la sencillez del mismo y el grado de impacto que puede tener, conocer esas debilidades, fortalezas, amenas y oprtunidades que mas adelante se traduce en benficio y organización empresarial para el logro de metas.

Espina de Pescado

La espina de pescado, diagrama de causa- efecto o digrama de Ishikawa que en el caso de esta última se debe a su creador Karou Ishikawa en 1943, al igual que la matriz DOFA pretende mejorar los procesos y calidad dentro de la organización, la diferencia con relación a la herramienta mencionada es que se identifican causas de un problema central.

Es una herramienta que analiza las causas que producen los fenomenos o tambien llamados problemas, es necesario decir que las causas no son depositadas de manera independiente si no que estas se vinculan entre sí. Las causas para el creador del diagrama se convierten en procesos que en terminos empresariales no solo es la creación de un producto si no factores que tambien hacen posible el producto, las cuales pueden ser los colaboradores, altos mandos, ambiente, coordinadición, dirección entre otros. (Ishikawa, 1993 citado en Campos, 2021, p.16)

En base a las causas existen categorias de estas y son materiales, mano de obra, metodo, ambiente maquina y medida.ahora bien como se habia mencionado en el parrafo anterior al convertirse las causas en procesos, es necesario tener un control de estas si se quiere tener efectos postivos. (Ishikawa, 1993 citado en Campos, 2021, p.16). En efecto las ventajas de la espina de pescado, es que el efoque es igual al problema, busqueda razonable de causas,y comprensión del problema por parte del equipo, quienes ayudan a la construcción del mismo. (Mayen et al., 2018 citado en campos, 2021, p.16).

Mapa de Empatía

El Mapa de Empatía es una herramienta que llama la atención porque posibilita ampliar el espectro que se tiene a la hora de crear servicio. Por ende, cuando se piensa en la idea de un producto más allá de la satisfacción del cliente, se busca es que le guste al cliente, por eso en diversas ocasiones se trabaja en base a percepciones individuales a futuro. Conviene decir que, el mapa de empatía permite conocer al usuario desea y busca de un servicio, teniendo en cuenta la parte sentimental y el comportamiento de los sujetos dentro de la sociedad, creando así una propuesta de valor en pro del cliente, tal y como se puede ver reflejado en la empresa XPLANE

quienes desarrollaron el término y dan prioridad a actos, actitudes, y visión del cliente (García L., 2019, p. 7).

Con el mapa de empatía se tendrá un buen modelo de negocio, los clientes orientaran esas propuestas de valor, que están en función de relaciones relativamente propicias. En definitiva, da a entender el por qué los clientes pagan por los productos (Osterwalder y Pigneur, 2011 p.131citado en García L., 2019, p.7). En otra instancia resulta interesante mencionar que la herramienta busca saber quién es el cliente, que necesita hacer, que escucha, que ve, que dice, que hace y sus esfuerzos (García L., 2019, p 8-10).

El diagrama de Pareto

Esta herramienta facilita hallar el problema principal, sin dejar de lado el análisis de la causa que genera dicho problema, hace pensar que tiene un grado de similitud a la espina de pescado que precisamente busca saber conocer causas. Cabe entonces decir que el diagrama de Pareto tiene un carácter de priorización de fenómenos entendiendo, recursos y medios con los que se cuenta. Entre tanto Pareto también suele conocerse como la ley 80/20 donde el 20% generan aspectos positivos en el 80% (Gutiérrez & De la vara, 2016 citado en Bolaños, 2019, p.3).

Juicio de Expertos

Teniendo en cuenta la visión del presente proyecto que respecta al diseño de un SGSI, sin duda el juicio de expertos se convierte en la opción más viable, menciona (Hernández et. al., 2016, p. 329)"la utilización de un juicio de expertos, como parte del proceso de rigurosidad metodológica brinda confiabilidad a los contenidos"

Él es válido de la información está vinculado a la muestra que habla de la totalidad de la población y de sus comportamientos con relación a medible, se hace necesarios profesionales en

temas afines o bien llamados juicio de expertos que según (Cuervo & Martínez, 2008 citado en Hernández et. al, 2016, p.330) “se define como una opinión informada de personas con trayectoria en el tema, que son reconocidas por otros como expertos cualificados en éste, y que pueden dar información, evidencia, juicios y valoraciones”

Marco Histórico

A continuación, las técnicas, instrumentos y herramientas que se han implementado en proyectos o investigaciones a través del tiempo para dar garantías adecuadas a los procesos de la entidad**.**

En primera instancia resulta indispensable mencionar el proyecto que lleva por nombre diseño e implementación de un SGSI, para el área de sistemas de la empresa ARFUSOG, bajo la norma técnica ISO -27001; el mismo servirá como herramienta para la gestión de la empresa. Por lo tanto, el diseño de un SGSI debe ir acompañado de un ciclo PDCA, basado en la clasificación de la información, la identificación de debilidades y amenazas a los activos de información y la evaluación de los peligros del sistema, lo que lleva a la definición de controles, política del sistema y documentos relacionados con el proceso de implementación y seguimiento de la mejora continua.

Cabe señalar que, a partir del año 1950, y en momentos posteriores, el autor Edward Deming utilizó el Ciclo PHVA, como una parte esencial de las capacitaciones brindadas a los líderes de empresas en Japón, sin embargo, el modelo o también llamado ciclo fue desarrollado por Shewhart, de manera que ha ido tomada relevancia en el mundo por sus implicaciones en la mejora Continua (García et. al, 2003, p.9).

Para ilustrar mejor la aplicación del ciclo PHVA, en el diseño e implementación de un SGSI en el dominio de TI, se considerarán 3 fases: en la primera fase, se establece un

compromiso con los gerentes de la empresa para comenzar a diseñar el sistema SGSI; en la segunda fase, se revisarán los elementos informáticos como hardware y software que utiliza una empresa para lograr sus objetivos y se definirán las personas responsables del proceso. En la tercera etapa se evalúan los riesgos identificados, sus impactos y se determinan los controles a implementar en el plan de riesgos.

Por consiguiente, se realiza un análisis periódico de la eficacia del SGSI implementado y los procesos inherentes al mismo. Resulta necesario decir que, se tiene en cuenta para la recolección de la información técnicas como la observación directa, la encuesta y la realización de pruebas. En la técnica de observación directa básicamente se revisa el inicio del sistema, la ubicación del servidor, el ingreso de datos, elaboración de copias de seguridad, actualización de información, manejo de correos electrónicos y contraseñas de acceso, ahora bien, para la técnica de la encuesta, se diseñó un cuestionario con preguntas cerradas el cual se aplicó a los colaboradores del área administrativa y operativa; se tomó en consideración variables como, tiempo, periodicidad, calidad, dificultades, reportes de fallas y nivel de satisfacción. De acuerdo con las pruebas, se realizaron escaneos o análisis de trafico de red, es decir que se revisa el funcionamiento de los sistemas cuando están operando, se concluye que la incidencia de un SGSI, en el área de informática trae grandes beneficios a mediano y largo plazo, para la protección de la información, igualmente, existe una contribución al fortalecimiento y estabilidad en el mercado del negocio, teniendo de base la disminución al máximo de los riesgos en la información. (Cordoba, 2015,pp.1-180)

Por otro lado, pero en la misma lógica de conocer acerca de herramientas o técnicas que han sido indispensable para el diseño de un SGSI, resulta necesario entonces mencionar que el proyecto llamado “Diseño de un sistema de seguridad la información **(**SGSI) para la asociación

ARFUSOG", Es causado por el modelo de gestión de seguridad de la información incompleto de la organización; para llevar a cabo el diseño del sistema, el proceso debe realizarse en etapas, como la etapa I de diagnóstico, la etapa II de preparación y la etapa III de planificación.

Tomando en consideración en la fase 1 Diagnóstico se pretende conocer la madurez de la organización con relación al sistema de seguridad de la información de la norma ISO/IEC 27001:2013, los mecanismos utilizados en esta etapa son cuestionarios sobre áreas de cumplimiento y estándares, documentación de calidad organizacional, roles y funciones de seguridad de la información relacionados con las partes interesadas y, por supuesto, guías y encuestas de autoevaluación.

En la fase 2 de preparación, en esta fase se llevan a cabo actividades como, establecer los documentos necesarios del SGSI, selección de herramientas y tecnologías para la gestión del riesgo, equipos de monitoreo de seguridad, soluciones de cifrado y autenticación, entre otros.

Con respecto a la fase III de planeación, en esta fase se establecen los objetivos, políticas, estrategias, procedimientos y procesos necesarios para garantizar la seguridad de la información en la organización, entre los cuales se pueden mencionar (identificación de activos de acuerdo con su criticidad y protección, valoraciones de los riesgos en cuanto al alcance, planes de acción y controles), entendiendo que existen objetivos para los controles determinados que reposan en un documento para tal función; dentro del contexto se debe elaborar un manual de políticas de seguridad de la información, que la organización aplicará como protección a la información.(Guzmán, 2015,p.42-73)

Es significativa la importancia que toman los registros documentales como herramienta para el diseño SGSI, en efecto, a la necesidad latente de no perder de vista información de gran relevancia; los registros documentales se convierten en la opción más viables ya que son una

fuente confiable donde se puede consultar datos, en el momento que el investigador considere vital, el hecho de que la información sea depositada, resulta practico, por temas de reportes, escritos, informes entre otros asuntos. (Bastar, 2012, p.45)

De acuerdo al parrafó anterior, hay dos tipos de registros documentales, las cuales son fichas de identificación y de investigación, en la primera se deposita información general de manera ordenada; con referencia a la segunda permite el registro de notas y la clasificación de la información. (Bastar, 2012, p.46-47)

Así como los registros documentales se han convertido en una herramienta eficaz para los investigadores, las encuentas tambien han tomado mucha relevancia si de investigaciones se trata; porque permiten ser aplicadas a un sin numero de personas y con variedad de temas al mismo tiempo, convien mencionar que según (Casa et.al, (2003)" En el ámbito sanitario son muy numerosas las investigaciones realizadas utilizando esta técnica, como queda demostrado en los 294 artículos encontrados en la base de datos Medline Express" (p.527).

Para García citado en Casa et. al (2003) la encuesta es un proceso estandarizado y bien estructurado, allí se recolecta información que va a hacer analizada posteriormente con relación a la población o muestra, sin embargo, una encuesta no sucede por si sola, sino que nace ante una necesidad, de explorar, describir, descubrir elementos o incluso explicarlos (p. 527).

Por otro lado, la herramienta de gestión de proyectos como es la matriz DOFA, compuesta por factores como (Debilidades, oportunidades, fortalezas y amenazas), básicamente busca determinar aspectos negativos y positivos de la empresa, es crucial decir que con la aplicación de la encuesta y el diagnostico se obtendrán elementos claves para el diseño del sistema SGSI.

Conviene decir entonces, que la información que quedó detallada en la matriz DOFA,

para el caso de las debilidades fueron, la ausencia de conocimiento de la norma técnica ISO-27001, reducida incidencia de los directivos de la empresa en el proceso, carencia de políticas de seguridad y falta de definición de roles. por consiguiente, en la parte de las fortalezas, se pueden implementar políticas de datos bien definidas que se comunique a los colaboradores de la empresa; la implementación de controles de acceso que protejan los activos de información.

Habría que decir también que, en las oportunidades quedo plasmada, certificación de la norma ISO 27001, incremento de la confianza en la agencia, políticas de seguridad de la información claras teniendo en cuenta manejo de esta, a su vez, queda claro la forma de proceder con respecto a la seguridad la información a través del tiempo. Prosiguiendo con el tema, dentro de las amenazas se plasmó, no contar con personal idóneo, pocos recursos económicos, poco compromiso para la implementación del SGSI, temas inherentes de la organización en la aplicación de apropiada de la seguridad. Con base al fundamento anterior, se contemplaron las estrategias DO, FO y DA, FA.

La estrategia (DO), se enfocará en aprovechar las oportunidades identificadas y superar las debilidades identificadas en el sistema de gestión de seguridad de la información de tal manera que se puedan desarrollar acciones para lograr los objetivos establecidos, esto puede incluir la asignación de recursos, la definición de responsabilidades y la elaboración de un plan de acción detallado con fechas límite para monitorear el progreso del sistema.

En cuanto a la estrategia FO, debe centrarse en aprovechar las oportunidades identificadas y utilizar las fortalezas del sistema de gestión de seguridad de la información. Para lograr esto, es importante identificar las fortalezas y oportunidades, desarrollar una estrategia clara y detallada, implementar la estrategia, monitorear la eficiencia del sistema, y evaluar los resultados para hacer ajustes si es necesario.

Con referencia a la estrategia DA, se deben enfocar en abordar las debilidades y mitigar las amenazas potenciales al sistema SGSI, ente estos tenemos la ausencia de capacitación y conciencia en seguridad de la información entre los empleados. Por último, pero sin restarle importancia a la estrategia FA, se centra en la necesidad en identificar fortalezas para disminuir amenazas que pueden afectar el sistema SGSI, es importante vincular a los empleados en la mejora del proceso. (Sierra & Cadena, 2017, pp. 37-38).

Entre tanto, se puede decir que, Aguila (2015), señala que en la tesis analisis de un sistema de gestión de seguridad de la información, basado en el criterio de la norma NTE INEN-ISO/IEC 27001: 2011, de un modelo de negocio aplicado.

En la comercialización y distribución de productos quimicos,utilizó la herramienta DOFA, precisamente para conocer las fortalezas, debilidades, oportunidades y amenazas como analisis estrategico, y queda expresado de la siguiente forma, en la fortalezas adecuado y consciente uso de la información, disminución de peligro respecto de la confiabilidad, integridad, y dispinibilidad de la misma. Si nos referimos a las debilidades la información expuesta fue carencia de conocimiento de la ISO 27001, igualmente demanda de capital para llevar un proceso de seguridad propicio (p.94).

En complemento, en las oportunidadescertificación de la norma NTE INEN- ISO/IEC 27001: 2011, además perfilación de la información con el modelo empresarial. Con respecto a las amenazas, conflictos internos al aplicar mecanismo de seguridad de la información adecuados (Aguila, 2015, p. 94).

Es oportuno ahora mencionar otra herramienta, la cual es el diagrama de pareto conocido tambien como la técnica 80/20 (factores determinantes y causas) en el análisis de la relación de costos- beneficio e implementación del sistema de gestión de calidad ISO 27001 en la empresa

GFI informática colombia S.A.S, no obstante, en los resultados hallados luego de la aplicación del diagrama de pareto, se menciona reducir los fallos funcionales y textuales, resulta etonces importate decir que si se trabaja estos dos aspectos, los otros aspectos negativos se pueden solucionar con inmediatez, en efecto, no es tan facil la solución, porque son aspectos aislados. Sin emabrgo cualquiera que fuese su solución, el diagrama de pareto busca conocer de ante mano el error más latente en el sofward y reducción en el tiempo de su realización.

De manera que el beneficio de la certificación en alta calidad se dará en el cumplimiento de la normatividad actual, en la realización procesos como soporte, garantía y seguridad ante los consumidores, que sirve de base para el estatus de la empresa en el mercado (Rincón, 2018, pp. 30-31-41).

Conviene deternernos a pensar en el diagrama de empatia como herramienta en la organizaciones, cabe señalar que Maderuelo afirma que "una empresa que no practica la empatía no conocerá las preferencias y gustos de sus consumidores. Para poder generar una oferta adecuada, es necesario conocer a tus clientes; probablemente falles una y otra vez". Se debe agregar que la empatia no solo esta en función del conocimiento de los clientes, de sus gustos, preferencias, incomormidad y demás, esta trasciende como aspectos, social, cognitivo, donde se permite situar en el otro respecto de las actitudes, comportamientos, sentimientos, emociones y generar a partir de ello respuestas acordes (Madurelo citado en Emprende hoy, 2017).

Es significativo mencionar que la empatía es un aspecto a desarrollar, tanto por la direccion de la organización, colaboradores, de manera que ello habla de la organización y su imagen (Mayen G. C., 2018, p.10). Por otra parte la herramienta espina de pescado tambien resulta ser un instrumento vital en el desarrollo de proyectos de diversas indoles y empresas, sin emabargo tambien es conocida como diagrama shikawa o diagrama de causa y efecto que en el

caso de esta última se busca lograr precisamente. En efecto “En una Aplicación práctica que utiliza los diagramas de Ishikawa para determinar las causas y plantear las posibles soluciones a los problemas identificados en las actividades logísticas de una empresa” (Domingos et. al, 2015, citado en Bernal, 2018, p. 58).

Finalmente, en cuanto a el jucio de experto, se define según, Escobar & Cuervo (2008) citado en Robles & Rojas, 2015, p.2). “como una opinión informada de personas con trayectoria en el tema.

Que son reconocidas por otros como expertos cualificados en éste, y que pueden dar información, evidencia, juicios y valoraciones”. Ahora bien, funciona de manera estrategica para todo el tema de evaluaciones, de la misma forma es sinonimo de ventaja, sin dejar de lado la extendida información del tema a trabjar y las observaciones de los profesionale. En concreto los expertos pueden ser escogidos por grados de afinidad entre el investigar y el experto, puede ser que no tenga ningun criterio de seleción o por medio de pruebas de coeficiente de competencia experta (Cabero & llorente, 2013 citado en Rojas, 2015, p.3).

Estado del Arte

Según menciona (Yuga y Narvaez, 2022), en su articulo, Aplicación de la Norma ISO-27001 para la seguridad de los sitemas de información.

La seguridad de datos y la información de cualquier tipo en la actualidad se ha convertido en un reto dentro de una organización. Un SGSI (Sistema de gestión de la seguridad de la información) hace que los riesgos de seguridad de la información para las organizaciones sean calculables y manejables. Mientras que la norma ISO 27001 proporciona un conjunto de controles para la seguridad de la información que una organización debe implementar en función de los resultados de una evaluación de riesgos y los requisitos de las partes interesadas. Es decir,

para cada riesgo a tratar se implementará una combinación de diferentes tipos de controles. Para la implementación de la norma ISO 27001 recurre a ciclo de Deming que se encarga en el continuo mejoramiento de la seguridad de la información. Podemos concluir que. Un SGSI actúa como un eje centralizado para salvaguardar y gestionar toda la información de una organización en un solo lugar. (p.1).

Por otro lado (Razikin y Soewito (2022), en el artículo Modelo de soporte de decisiones de ciberseguridad para diseñar un sistema de seguridad de tecnología de la información basado en el análisis de riesgos y el marco de ciberseguridad, El modelo propuesto tuvo como objetivo: obtener el mejor sistema de seguridad para mitigar las amenazas a la seguridad. Este documento contribuyó a los formuladores de políticas estratégicas en el diseño de recomendaciones de soporte de decisiones de seguridad cibernética para determinar los mejores pasos en el diseño de sistemas de seguridad de tecnología de la información. El modelo construido puede mapear el valor de prioridad de la mitigación de amenazas en función de la puntuación de amenaza relativa frente a la puntuación de evaluación relativa de la implementación del cumplimiento de ISO/IEC 27001. (p.1).

En relación con el SGSI, (Mora et al.,(2020), en su artículo llamado El sistema de gestión de seguridad de la información bajo la norma NTE ISO/IEC 27001 en instituciones de Educación Superior; el cual tenía como objetivo:

Describir una metodología para un Sistema de Gestión de Seguridad de la Información (SGSI) para instituciones de educación superior del Ecuador, bajo la norma NTE INEN-ISO/IEC 27001, la cual será de utilidad en el momento de su aplicación y facilitará el desarrollo de las fases del ciclo PHVA (Planear, Hacer, Verificar y Actuar) a nivel institucional. Se tomó como referente a la Universidad Técnica Estatal de Quevedo (UTEQ), se identificaron los procesos

claves de la universidad estudio de caso, se identificaron y clasificaron los activos de información y controles que permitieron contextualizar los alcances del SGSI, que permitirán a la UTEQ organizar, diseñar y gestionar de manera sistemática su SGSI, plantear estrategias de cambio y mejora, valorar y asegurar sus activos de posibles riesgos y vulnerabilidades. (p1)

Vargas (2019), Presentaron el, Diseño de un sistema de gestión de seguridad de la información para la empresa caso de estudio QWERTY S.A. A través de la planeación empresarial garantiza el cumplimiento de las políticas de seguridad de la información definidas en el presente manual, buscando el mejoramiento continuo del sistema, toda la organización deberá velar por el cumplimiento de la política de seguridad basada en las buenas prácticas y fortalecimiento de los procesos de cada una de las áreas de la entidad, verificando constantemente el seguimiento mediante auditorías internas sobre el estado de implementación y madurez del sistema de gestión de seguridad de la información, elaborando los respectivos planes de mejora continua.(p.183)

Guzmán C (2015) diseñó un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso (IGM S.A), basado en la norma NTC-ISO-IEC 27001:2013: El propósito era proporcionar los elementos, mecanismos y directrices necesarios para mejorar los procesos de la entidad y el manejo de los riesgos asociados con el uso de la información. Además, se buscó establecer un Gobierno de Seguridad que estuviera alineado con la cultura organizacional, las necesidades y los objetivos del negocio. Esto se logró mediante una estructura organizacional con roles y responsabilidades claras, y un conjunto coherente de políticas, procesos y procedimientos. El objetivo final era fomentar y extender una cultura de seguridad en todos los niveles de la organización.

Mendoza D (2019) presentó una propuesta sobre la importancia de implementar un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO 27001 en las empresas.

En esta propuesta, se utilizó el ciclo PHVA para desarrollar el sistema de gestión de seguridad de la información, lo que permite a la organización prepararse para un mercado competitivo donde se requiere un mejoramiento continuo en altos niveles de calidad. A pesar de que esta herramienta (DEMING) es antigua, sigue siendo relevante ya que integra los elementos básicos e imprescindibles para el desarrollo.El punto de partida para la implementación de un sistema de gestión es contar con el apoyo de la alta dirección para llevar a cabo un diagnóstico inicial. Luego, se debe definir el alcance y establecer objetivos. Es esencial contar con un equipo altamente capacitado y un cronograma con las actividades a realizar. Es importante destacar que todos los empleados deben conocer la cultura organizacional de la empresa para que el sistema tenga madurez.

Guaman y Cárdenas (2022), en el estudio realizado al SGSI identificaron que tiene como fin. Determinar el grado de cumplimiento de las políticas de seguridad de la información en las cooperativas de ahorro y crédito del Cantón Cañar, segmento 3, la metodología utilizada tiene un enfoque cuantitativo de carácter descriptivo y explicativo, se usa la norma ISO 27001:2013 y la guía de buenas prácticas ISO 27002 con el fin de evaluar cada uno de sus dominios y objetivos de control. El sustento teórico se lo realiza analizando documentos que explican sobre el Sistema de Gestión de Seguridad de la Información (SGSI), ISO 27000, Ley Orgánica de Economía Popular y Solidaria (LOEPS) y la normativa que emiten los organismos de control de referencia a la seguridad de los sistemas de información. Para determinar la situación actual de las cooperativas se aplicó una encuesta a los responsables del departamento de tecnologías de la

información para evaluar cada uno de los dominios. Los resultados indican que existen dos dominios con riesgo bajo, seis dominios tienen riesgo medio y seis dominios con riesgo alto. (p.1)

Según menciona (Martin, 2021), en el artículo, llamado Automatización de un sistema de gestión de Seguridad de la Información basado en la norma ISO-IEC 27001. El presente trabajo tiene como objetivo describir los requisitos para la implementación y la documentación necesaria de un Sistema de gestión de seguridad de la información (SGSI). La automatización consiste en la disponibilidad de una plantilla con preguntas de control internas enfocadas en los 3 pilares de la seguridad de la información (confidencialidad, integridad, disponibilidad) que permita realizar un "Gap-Analysis" para medir el nivel de madurez actual respecto a los requisitos del estándar internacional ISO/IEC 27001:2013, con un diagrama de radar y así instaurar un SGSI o realizar el proceso de la certificación ISO 27001 que garantice minimizar el riesgo y proteger la información en las computadoras o en los sistemas interconectados, ya que es uno de los activos más importantes de las organizaciones, asegurar la confidencialidad e integridad de los datos y de la información de determinados procesos críticos o sensibles, cuya pérdida, fuga o no disponibilidad de la información pongan en problemas a la organización. (p.1)

(Guerra et al. 2021), el objetivo principal de este estudio de investigación es aplicar un sistema de gestión de la información basado en la metodología de análisis e identificación de riesgos para los procesos de las bibliotecas universitarias. Se adapta y aplica la norma ISO/IEC 27001:2013 utilizando la metodología MARGERIT para evaluar una biblioteca universitaria.

Los resultados obtenidos de los cálculos de riesgo intrínseco y efectivo muestran la presencia de salvaguardas y la evaluación de impactos. Se establece el porcentaje de influencia en cada riesgo por proceso de calidad, se identifican medidas correctivas y se incorporan

formatos de registro. Se concluye que la incorporación de los formatos propuestos para desarrollar controles y auditorías de indicadores de calidad permiten optimizar el sistema de gestión de seguridad de la información (SGSI) de los procesos bibliotecarios universitarios. (p.1)

En relación con el SGSI, (Yungan et al.(2022), menciona que. La seguridad de datos y la información de cualquier tipo en la actualidad se ha convertido en un reto dentro de una organización. Un SGSI (Sistema de gestión de la seguridad de la información) hace que los riesgos de seguridad de la información para las organizaciones sean calculables y manejables. Mientras que la norma ISO 27001 proporciona un conjunto de controles para la seguridad de la información que una organización debe implementar en función de los resultados de una evaluación de riesgos y los requisitos de las partes interesadas. Es decir, para cada riesgo a tratar se implementará una combinación de diferentes tipos de controles. Para la implementación de la norma ISO 27001 recurre a ciclo de Deming que se encarga en el continuo mejoramiento de la seguridad de la información.

Marco Legal

A continuación, se realiza una descripción del marco legal, que se aplicara según las leyes normas o lineamiento de las instituciones reguladoras en Colombia, para dar solución a la problemática asociada al presente estudio de investigación acerca del sistema de gestión de la seguridad de la información (SGSI). De acuerdo con las ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente (Técnica NTC-ISO/IE CColombiana 27001, 2006-03-22, 2006-03-22).

El Decreto 1360 de 1989 señala que "Por medio del cual se reglamenta la inscripción de soportes logístico (software) en el registro nacional de derechos de autor". El artículo 4°**,** soporte lógico (software), será considerado como obra inédita, salvo manifestación en contrario hecha por el titular de los derechos de autor (El Presidencia de la Republica de Colombia, 1989)

De acuerdo con la Ley 527 de 1999 "por medio de la cual se definen, reglamenta el acceso, uso de los mensajes de datos, del comercio electrónico, de las firmas digitales, se establece las entidades de certificación y se dictan otras disposiciones.

Acuerdo sobre el uso del mecanismo de firma electrónica: Acuerdo de voluntades mediante el cual se estipulan las condiciones legales y técnicas a las cuales se ajustarán las partes para realizar comunicaciones, efectuar transacciones, crear documentos electrónicos o cualquier otra actividad mediante el uso del intercambio electrónico de datos (El presidente de la República de Colombia, (Noviembre 22 de 2012)).

Ley 1266 de 2008 señala en el Artículo 2°. Ámbito de aplicación. La presente ley se aplica a todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada.

De acuerdo con el artículo 4° en el principio de la administración de datos. f) Principio de seguridad. La información que conforma los registros individuales constitutivos de los bancos de datos a que se refiere la ley, así como la resultante de las consultas que de ella hagan sus usuarios, se deberá manejar con las medidas técnicas que sean necesarias para garantizar la

seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado (Colombia, congreso de la república., Diciembre 31 de 2008).

Metodología

Diseño de un sistema de Gestión de seguridad de la información (SGSI) para la asociación ARFUSOG, recolectora de residuos sólidos de la ciudad de Sogamoso, mediante el uso de herramientas de gestión de proyectos

Tipo y Enfoque de Investigación

El presente proyecto se realizará bajo una metodología mixta, basado en el enfoque descriptivo, ya que la investigación tiene como propósito definir, clasificar y lograr la caracterización detallada de la situación o problema objeto de estudio para ser analizada.

Instrumento de Recolección de Información

Como instrumento de recolección de información se seleccionó el cuestionario ya que es una herramienta que permite obtener información de manera rápida y directa de los sujetos de estudio con el fin de lograr resultados óptimos. El cuestionario estará compuesto de preguntas cerradas con única respuesta.

De la misma manera se utilizará el análisis a través de un diagnóstico el cual se realizará a través de las herramientas de gestión de proyectos como la espina de pescado, el diagrama de Pareto y la matriz DOFA.

Muestra

La muestra seleccionada corresponde a la unidad debido que se realizó un muestreo no probabilístico, porque se va a trabajar con una sola empresa, que cuenta con 9 empleados a los cuales se les aplicara la encuesta.

Procedimiento de la Metodología

Diseño de un sistema de Gestión de seguridad de la información (SGSI) para la asociación ARFUSOG, recolectora de residuos sólidos de la ciudad de Sogamoso, mediante el

uso de herramientas de gestión de proyectos. Para el desarrollo del proyecto Diseño de un sistema de Gestión de seguridad de la información (SGSI); se realiza la exploración bibliográfica para así definir los elementos que más se ajuste al desarrollo del SGSI.

Fase 1. Diagnóstico del Sistema SGSI

Etapas 1. Consecución de la Información Directa

Tareas 1**.** Obtención de la información del sistema de estrategias de seguridad de la información de una empresa recolectora de residuos, mediante la revisión de la base de datos de la empresa, a través de la entrevista, al personal del área administrativa y operativa, con el fin de determinar información del diagnóstico.

Tarea 2**.** Análisis de la información del sistema de estrategias, por medio de una herramienta Excel, para analizar información del diagnóstico.

Tarea 3. Desarrollo de la encuesta para obtener información estratégica del SGSI, mediante datos; a fin de usar el instrumento de la encuesta.

Tarea 4. Recopilar y conocer las opiniones de los empleados de la empresa a través de la aplicación del mapa de empatía.

Tarea. 5. Creación y aplicación de la encuesta con la finalidad de obtener información del sistema de estrategias de seguridad de la información por medio del formulario Google.

Tarea. 6. Análisis de la encuesta mediante la matriz DOFA

Tarea 7. Síntesis de las herramientas aplicadas (Encuesta, mapa de empatía y matriz DOFA)

Fase 2. Análisis del diagnostico

Etapa 3. Análisis del resultado de la encuesta y el diagnostico

Tarea 8. Análisis del sistema de Seguridad de la información mediante el uso de la matriz DOFA, con el fin de determinar las debilidades, oportunidades, fortalezas y amenazas.

Tarea 9. Síntesis de las oportunidades de mejora del SGSI, para hallar posibles soluciones.

Etapa 4. Análisis de las debilidades del sistema de Gestión de seguridad de la información través de herramientas de gestión de proyectos.

Tarea 10. Análisis las debilidades del SGSI; mediante de la espina de pescado, Diagrama de Pareto y los 5 porqués, para generar propuestas en la optimización del sistema.

Tarea 11. Análisis Alternativas de solución mediante la herramienta lluvia de ideas

Tarea 12. Síntesis de las herramientas de gestión de proyectos aplicadas al problema objeto de estudio de la asociación ARFUSOG, para determinar las posibles soluciones.

Fase 3. Valoración de Alternativas de Solución

Etapa 5. Estimación posibles soluciones del Sistema de Gestión de Seguridad de la Información por Medio del uso de Herramientas de Gestión de Proyectos

Tarea 13. Evaluación de las soluciones y propuestas de mejoramiento del SGSI, mediante el uso de una matriz de priorizaron y juicio de expertos, para determinar la mejor solución según el sistema de información.

Tarea 14. Utilización de la norma técnica ISO-27001, literal (a) enfoque basado en procesos de planificación SGSI, con la finalidad de establecer los requisitos y controles de mejora del sistema de seguridad de la información de la empresa asociación ARFUSOG.

Tarea 15. Definición los activos a proteger en el sistema de Información SGSI

Tarea 16. Definición los responsables de la seguridad de la Información para ARFUSOG

Tarea. 17. Establecimiento de las Políticas de seguridad de la Información para la empresa ARFUSOG

Tarea. 18. Requisitos de documentación

Tarea. 19. Recursos necesarios para la operación, mantenimiento y mejora del sistema SGSI

Tarea. 20. Síntesis de las alternativas de solución a nivel técnico y económico

Etapa. 6. Conclusiones

Etapa. 7. Recomendaciones

Las herramientas de gestión de proyecto seleccionadas para el desarrollo de esta investigación son el mapa de empatía, la matriz DOFA, el diagrama de Pareto y la espina de pescado. A continuación, se describe la finalidad de cada una de las herramientas de gestión de proyectos para el análisis del Sistema de Seguridad de la información SGSI de la empresa

ARFUSOG:

El mapa de empatía permite conocer de manera detallada que el usuario desea y busca de un servicio, de esta manera la empresa puede crear una propuesta de valor en pro del cliente.,

Matriz DOFA, permite realizar un análisis de los factores internos y externos de la empresa, de tal manera que se pueda hacer una evaluación de las debilidades, fortalezas, amenazas y oportunidades del sistema de información de la empresa.

El diagrama de Pareto se utiliza comúnmente en el contexto del SGSI para identificar los principales riesgos de seguridad de la información, porque muestra la frecuencia de los problemas o causas de problemas en orden descendente, que ayuda a la organización a centrarse en los problemas más importantes y abordarlos de manera efectiva.

Espina de pescado tiene como finalidad identificar las causas y del sistema de información de la empresa.

Diagnóstico del Sistema SGSI

Consecución de la Información Directa

En esta etapa se determinará la consecución de la información con el fin de determinar información del diagnóstico descritas a continuación:

Determinación de la Información del Diagnóstico Preliminar

En el mundo empresarial el éxito no depende solo del producto o servicio que se ofrece al cliente si no de un conjunto de procesos y objetivos misionales de la organización que permitan la competitividad en el entorno para sostenerse en el tiempo. De igual forma se hace necesario vincular procesos de la entidad a los activos intangibles como es el flujo de información, su confidencialidad, integridad y disponibilidad de esta.

Por consiguiente, se hace necesario realizar un análisis del Sistema de Seguridad de la Información SGSI de ARFUSOG, mediante la herramienta Excel en la cual se diseñó un cuadro que contiene una columna con preguntas, otra con respuestas cerradas, a la persona entrevistada y por último relaciona observaciones finales donde se justifica la respuesta dada por cada uno de los funcionarios de la empresa.

A continuación, se relaciona la tabla 1, de la entrevista realizada al personal administrativo y de la empresa asociación ARFUSOG.

Tabla 1

Entrevista Estructurada del Sistema de Gestión de ARFUSOG

Entrevista al personal administrativo de la empresa ARFUSOG para el Sistema de Seguridad de la Información			
Preguntas	**Respuestas**		**Observación**
	Si	**No**	
¿La empresa está conformada legalmente?	X		La empresa cuenta con cámara de comercio y Rut
¿La empresa maneja software administrativo, contables y de inventario?	X		La empresa cuenta con un software contable y de inventarios que soporten la información financiera e inventario de la empresa.
¿Tiene un manual documentado para realización de los procesos, procedimiento y política de la empresa?		X	La persona encargada del manejo de los documentos es la secretaria, quien guarda información en archivo físico soportado en un documento en Excel
¿La empresa cuenta con una estructura organizacional?	X		La empresa cuenta con 9 empleado
¿Cuenta la empresa con un sistema de gestión de la información digital o físico?		X	La información se relaciona en un archivo en Excel
¿Cuenta la empresa con una matriz de responsabilidades en cuanto al manejos de claves y contraseña para acceder de la información de la empresa?		X	Cada persona es responsable de guarda en su pc y / o en documentó físico que le son asignados

¿Cuenta la empresa con personal capacitado para realizar el archivo y selección de los documentos de la empresa?		X	El aprendizaje ha sido empírico
¿Se cuenta con un comité interno para establecer las políticas de Seguridad de la información?		X	La empresa no tiene conocimiento que se puede elegir un comité para el diseño de político de seguridad de la información
¿Se cuenta con Tecnología para evitar y responder a amenazas Cibernéticas?		X	La empresa no cuenta con un sistema de detención de amenazas cibernéticas, pero tiene la disposición de implementar esa tecnología en la empresa.
¿Se cuenta con Tecnología para el respaldo y Recuperación de la Información		X	La información se almacena en un disco duro y memorias USB
¿Tiene usted conocimiento de la ISO 270001?		X	La empresa no cuenta con un SGSI, pero tiene la disposición y desea implementarlo en la empresa
¿Los empleados de la empresa utilizan correo electrónico institucional?	X		La empresa cuenta con un dominio para sus correos institucionales: aprovechamiento@arfusogsbc.com
¿cuenta la empresa con misión y visión?	X		**Misión:** Mejorar la calidad de vida de los asociados y sus familias mediante la inclusión y dignificación del gremio reciclador, contribuyendo a la conservación del medio ambiente y así mismo educar a la comunidad Sogamoseña en la cultura del reciclaje. **Visión:** Para el año 2025 ARFUSOG será la organización líder en prestación del servicio

	público de aprovechamiento en la ciudad de Sogamoso, optimizando su esquema operativo, convirtiéndose en una empresa sostenible con presencia y reconocimiento a nivel nacional e internacional, contribuyendo al cuidado del medio ambiente.

Nota. **E**laboración propia

A partir de la entrevista estructurada realizada al personal administrativo, como se indica en la tabla 1, se obtuvo una información inicial del Sistema SGSI de ARFUSOG; en la cual las personas entrevistadas manifestaron que la empresa desconoce la norma técnica ISO-27001, de la misma manera carece de políticas definidas para sistema de seguridad de la información, la documentación se maneja en archivo físico, no existe claves o contraseñas de acceso a la información quedando expuesta al alcance de terceros, además no existe un RAP que almacene la información compartida con disponibilidad, integridad y confidencialidad; contrario a esto la información se almacena en memoria USB.

En segunda instancia con la finalidad de profundizar en el análisis del sistema SGSI, se compartió una encuesta al personal administrativo y operativo de la organización a través de un formulario Google, el cual consta de preguntas de selección múltiple con única respuesta, (ver encuesta en anexo 1).

Sistema de Estrategias por Medio de una Herramienta Excel, para Analizar Información del Diagnóstico

A través de la herramienta Excel, se realizará un análisis detallado de cada uno de los archivos y documentos de la empresa a partir de la entrevista realizada al personal administrativo y operativo de la asociación con la finalidad de determinar el diagnóstico y profundizar en el sistema de seguridad de la información de esta.

Desarrollo de la Encuesta como Instrumento Recolección de Información

Para el análisis de la información en el diseño de las preguntas de la encuesta, se aplicó la herramienta mapa de empatía, porque establece una visión global del usuario interno, permite conocer su personalidad, su entorno, necesidades y deseos con respecto a la empresa.

Recopilación y Reconocimiento de las Opiniones de los Empleados

El diagrama de empatía consta de seis partes que representan problemas, deseos y demandas de las personas hacia la empresa; las preguntas que conforman el diagrama son las siguientes; ¿Que ve?; ¿Qué dice y que hace?; ¿Qué oye ?; ¿Qué piensa y que siente?; ¿Cuáles son los esfuerzos que realiza?; ¿Cuáles son los resultados y beneficios que espera obtener?, tal y como se observa en la figura 1 Análisis de la encuesta a través del mapa de empatía.

Inicialmente el diagrama de empatía permite evaluar de manera constante los segmentos del modelo de negocio e identifica procesos tradicionales y ayuda a generar estrategias para adicionar a la empresa nuevos procesos innovadores, de tal manera que cree una ventaja competitiva que responda a las necesidades de los clientes dejando de lado los esquemas tradicionales y fomentando el desarrollo para crear el valor agregado a nivel interno y externo.

Cabe resaltar que la opinión del cliente solo es un punto de partida que amplía el espectro para iniciar un proceso de innovación, tal y como se muestra en la figura 1 Mapa de empatía.

Figura 1

Análisis de la Encuesta a través del Mapa de Empatía

Nota. Elaboración propia. *Fuente.* Mapa de empatía (Herramienta diseñada por XPLANE)

En la tabla 1, Se observan los resultados de la entrevista aplicada al personal administrativo y operativo de la empresa, en las cuales se realizó un análisis detallado de las diferentes situaciones que afectan la seguridad física, que permitió identificar problemas relacionados con la falta de información sobre el diseño de sistemas de gestión de seguridad para mantener la confidencialidad, integridad y disponibilidad de la información de la empresa.

Después de recopilar información a través del mapa de empatía se procede a diseñar una encuesta mediante el formulario Google, con la finalidad de ampliar información del problema objeto de estudio.

Creación del Instrumento y Aplicación de la Encuesta

En esta fase se crea el instrumento de recolección de información a partir de datos registros y entrevistas realizadas al personal administrativo de la empresa, tal como se observa en la tabla 1 y en la encuesta del formulario Google (https://forms.gle/ERsZEEqXp6uJPjA28).

La encuesta es aplicada a los 9 empleados que tiene la empresa en sus áreas operativas y administrativas, la muestra seleccionada para la aplicación de la encuesta se conoce como muestreo por conveniencia o técnica de muestreo no probabilística donde los actores de la población se seleccionan por su disponibilidad y facilidad de acceso para la recolección de información.

Los resultados del sistema de gestión de ARFUSOG, permitieron el análisis de los factores internos y externos; primero se analizaron las amenazas como factor negativo que puede afectar los objetivos misionales de la organización; segundo se determinan las oportunidades como factor positivo a nivel externo de la empresa que se puede aprovechar para mejoras continuas de los procesos de la organización; tercero identificación de fortalezas como aspectos positivos a nivel interno de la empresa en cuanto a capacidades y habilidades del personal y la maquinaria instalada; cuarto identificación de las habilidades como factor negativo a nivel interno de la organización que obstaculizan el logro de objetivos.

Análisis de la Encuesta Mediante la Matriz DOFA

Se aplico la encuesta al personal administrativo y operativo de la empresa asociación ARFUSOG, la cual se puede visualizar en el anexo 2 del trabajo.

La encuesta aplicada arrojo como resultado que el 89% de los empleados de ARFUSOG, no tienen conocimiento de la norma técnica ISO-27001; por lo cual es preciso establecer los

requisitos de seguridad de la información del negocio, y la necesidad de establecer la política y objetivos en relación con la seguridad de la información de la empresa.

Por consiguiente, es necesario establecer un sistema SGSI, porque el 88,9 % de los empleados no tienen conocimiento sobre el sistema de seguridad de la empresa, se hace necesario que la empresa establezca políticas de procedimiento para la disponibilidad, confidencialidad e integridad de la información. Esto garantizara que solo las personas con autorización y claves de acceso pueden acceder a la información de la organización.

Cabe resaltar que el 68% de los empleados manifiestan que las copias de seguridad de la información la hacen ellos a través de memorias USB, estos dispositivos corren un riesgo grande de perdida de la información y virus a archivos que limita el acceso de la información al usuario. Se deduce que la empresa no tiene una cultura de seguridad de la información establecida que le permita tener un control de los procesos y procedimientos para el acceso a la información por parte de los usuarios internos y externos.

A partir de la aplicación de la encuesta al personal administrativo y operario, por medio de la DOFA se identificaron las Amenazas, fortalezas, debilidades y oportunidades de la empresa a nivel interno y externo, se convierte en un elemento fundamental para la toma de decisiones de la organización. A continuación, en la tabla 2 análisis del diagnóstico se describen las debilidades, oportunidades, fortalezas y amenazas.

Tabla 2

Análisis del Diagnóstico Mediante la Matriz DOFA

Matriz DOFA		
	Debilidades	**Oportunidades**
1. Factores externos DOFA	Desconocimiento de la norma ISO 27001 Falta de implementación de políticas y procedimientos para guardar la información Sin definir los responsables de accesos, rutas y contraseñas para acceder a la información Archivo físico	Certificación ISO 27001 Establecer políticas, procedimientos y definir responsables de la seguridad de la información. Establecer recursos necesarios para la operación, mantenimiento y mejora del sistema Aplicaciones de controles de seguridad Sistematizar la información
	Amenazas	**Fortalezas**
2. Factores Internos DOFA	Desconocimiento para el manejo del archivo Perdida de la información Ataques cibernético Falta de recursos para implementar un SGSI Resistencia por parte de los empleados para implementar el Sistema SGSI	Disponibilidad de la Gerencia para iniciar un sistema SGSI.
Estrategia FODA		
FO (Fortaleza – Oportunidad)	Aprovechar la disponibilidad de la gerencia de ARFUSOG para establecer las políticas y procedimientos del SGSI	**DO (Debilidad – Amenaza)** Aplicar controles de seguridad de la información y sistematizar la información para evitar pérdidas y ataques cibernético
FA (Fortaleza – Amenaza)	Con el apoyo de la gerencia de la asociación capacitar al personal en el manejo de la información	**DA (Debilidad – Amenaza)** Inventariar y valorar los activos de la organización

Contratar personal con conocimientos en el manejo del sistema SGSI

Nota. Elaboración propia

Síntesis de las Herramientas Aplicadas (Encuesta, Mapa de Empatía y Matriz DOFA)

En cuanto a la Matriz DOFA detallada en la tabla 2 como diagnóstico de la encuesta aplicada a todo el personal de ARFUSOG, resultan unos hallazgos importantes con respecto a las debilidades como factor interno, se encuentra que los empleados del área administrativa y operativa desconocen la existencia de la norma ISO 27001, a su vez mencionan la falta de implementación de políticas y procedimientos que permitan salvaguardar la información de tal manera que permanezca disponible, íntegra y que sea confidencial, sin restarle importancia a que no hay responsables que briden el acceso y contraseñas de acceso a la información, aun manejan documentos en archivo físico, se representa un riesgo inminente para la empresa; de acuerdo con dicho anterior es vital tomar en consideración a la estrategia FODA y sus combinaciones que a nivel corporativo tiene pretensiones de mejorar tácticamente situaciones desfavorables para enrutar a la organización a tener un progreso significativo con el sistema de Seguridad de la Información.

Por consiguiente, conocer las debilidades permite explotar oportunidades entre las cuales se encuentra la certificación ISO-27001, establecer políticas y procedimientos, definir responsables de la seguridad de la información, precisar recursos necesarios para operación, mantenimientos, mejora continua de los procesos, capacitación al personal, aplicación de controles de seguridad y sistematización de la información, abriendo paso a las siguientes estrategias (Debilidades vs Oportunidad (DO), Debilidad vs Amenaza (DA), Fortaleza vs Oportunidad, Fortaleza vs oportunidad (FO), Fortaleza vs Amenaza(FA).

La estrategia Do se visiona a aplicar controles de seguridad de la información y sistematizar la información para evitar pérdidas y ataques cibernéticos por parte de terceros. Así mismo es prudente tomar en cuenta la estrategia DA, que además de contrarrestar debilidades contrarresta amenazas como factor externo donde se encuentra desconocimiento para el manejo de archivos, falta de recursos para implementar el SGSI, resistencia por parte de los empleados entre otros, en resumen, la estrategia busca inventar y valorar los activos de la organización sumando aspectos como contratación de personal con conocimiento en el manejo del SGSI.

Referente a las fortalezas, se descubre que la alta gerencia se muestra presta para la aplicación de un SGSI, no obstante, una estrategia que permite optimizar fortalezas para maximizar oportunidad es la FO por tanto se menciona que será necesario aprovechar la disponibilidad de la gerencia de ARFUSOG, de manera proactiva y sistemática para establecer las políticas y procedimientos del SGSI. Ahora bien, si de fortalezas se trata la estrategia FA no se queda atrás enfocándose en fortalecer y minimizar amenazas, desde el apoyo de la gerencia de la asociación para capacitar al personal en el manejo de la información.

Análisis del Diagnostico

Análisis del Resultado de la Encuesta y el Diagnostico

En esta etapa se determinará el análisis del resultado de la encuesta y el diagnóstico del sistema de seguridad de la información de la empresa descritas a continuación:

Aplicación de la Matriz DOFA, con el fin de Determinar las Debilidades, Oportunidades, Fortalezas y Amenazas del SGSI.

En la tabla 3 análisis de las debilidades encontradas en la asociación empresa ARFUSOG, se identificaron las estrategias con el objetivo de hacer una revisión interna y externa al contexto de seguridad y necesidades que tiene la empresa para implementar un sistema SGSI, por otro lado, en la revisión se halló la siguiente:

Primero la empresa necesita adoptar estrategias que le permitan aprovechar la disponibilidad de la gerencia para implementar un sistema SGSI; de la misma manera capacitar al personal en el manejo de la información; implementar nuevas estrategias tecnológicas como proceso de innovación y mejora continua que facilite la comunicación con clientes y proveedores para hacer más ágil el servicio.

Segundo ARFUSOG, no tiene claro que para enfrentar al entorno competitivo debe alcanzar los objetivos misionales, de tal manera que pueda convertir las debilidades y amenazas en oportunidades y fortalezas, todo esto con la finalidad de crear estrategias al contexto de seguridad a través de la implementación de procedimientos de control para el acceso de los usuarios internos y externos a los archivos de la organización.

Tercero la organización no tiene un inventario definido de los activos y el riesgo de vulnerabilidad de estos, de la misma manera no ha determinado un área que se encargue del mantenimiento de equipos y la asignación de roles y responsabilidades en cuanto al manejo del

Sistema de Seguridad de la información; por siguiente le falta una matriz de riesgos e impactos que faciliten el seguimiento a los procesos.

De acuerdo con los resultados de la matriz DOFA, ARFUSOG, tiene la necesidad de Implementar y estandarizar internamente procedimientos al sistema de datos para asegurar el cumplimiento normativo y la trazabilidad como mejora continua.

Todo lo anterior para reducir posibles riesgos o circunstancias que puedan afectar los objetivos misionales de la organización. Asimismo, desarrollar el sistema SGSI, mediante procesos de calidad y la eficacia en el desarrollo del objeto social, como se muestra en la tabla 3.

Tabla 3

Análisis de Debilidades Encontradas en el Diagnostico

Factores		Análisis debilidades Estrategia	Análisis	Beneficios de adoptar un sistema SGSI
Fortaleza	**Oportunidad**	**FO**	**Interno**	
1.Capacidad de enfrentar a la competencia	1.Certificacion ISO 27001 2. Establecer políticas, procedimientos y definir responsables de la seguridad de la información	1.Implementar estrategias para abrir nuevos nichos de mercado 2. Aprovechar la disponibilidad de la Gerencia para implementar un sistema Gestión de la Información	El análisis interno permitirá a la organización identificar sus capacidades y recursos para la mejora continua y de esta manera afrontar el entorno competitivo para alcanzar los objetivos propuestos.	Tener control de los activos de la empresa y los riesgos de vulnerabilidad de estos
2.Estabilidad laboral para los empleados	3. Definir recursos necesarios para la operación, mantenimiento y mejora del sistema			Disminuir la perdida de información y el acceso por parte de terceros
3.Disponibilidad de la Gerencia para automatizar la información	4. Aplicaciones de controles de seguridad 5. Sistematizar la información	**FA** 1. Con el apoyo de la gerencia de la asociación capacitar al personal en el manejo de la información	**Externo**	Reducir los riesgos en materia de confidencialidad, integridad y disponibilidad.
4.Personal con conocimiento del recorrido de las rutas	**Amenaza** 1.Personal no calificado para el manejo del archivo 2.Perdida de la información por ataques cibernético 3.Falta de recursos para implementar un SGSI	2. Implementar nuevas estrategias tecnológicas como proceso de innovación y mejora continua que permitan la	El análisis externo permite conocer las oportunidades y amenazas de la organización frente a la competencia, de esta manera la empresa puede	Implementación de políticas de seguridad de la información

	4.Resistencia por parte de los empleados para implementar el Sistema SGSI	comunicación con clientes y proveedores y la agilidad del servicio	diseñar estrategias que le permitan estar a la vanguardia de la economía cambiante	Cultura organizacional del tratamiento de datos
Debilidad	**Oportunidad**	**DO**	**Contexto de seguridad**	
1.Desconocimiento de la norma ISO 27001	1.Certificacion ISO 27001 2. Establecer políticas, procedimientos y definir responsables de la seguridad de la información	1.Aplicar controles de seguridad de la información y sistematizar la información para evitar pérdidas y ataques cibernético	ARFUSOG, ha implementado procedimientos de control en la seguridad de la Información, como correos institucionales, Software contable e implementación de la licencia del office. Sin embargo, a un está en proceso de mejora ya no cumple con los estándares que propone la norma ISO-27001	Determinar los roles, responsabilidades y accesos al sistema de información, para el manejo de información, registros y aprobaciones
2.Falta de implementación de políticas y procedimientos para guardar la información	3. Definir recursos necesarios para la operación, mantenimiento y mejora del sistema 4. Aplicaciones de controles de seguridad 5. Sistematizar la información	2. Crear una base de datos de clientes y proveedores 3. Crear un archivo digital con permisos y accesos para los colaboradores y directivos de la organización		Certificación ISO- 27001 Procesos documentados y automatizados
3.Sin definir los responsables de accesos, rutas y contraseñas para acceder a la información 4. Archivo físico	**Amenaza** 1. Personal no calificado para el manejo del archivo 2. Perdida de la información Ataques cibernético 3. Falta de recursos para implementar un SGSI 4. Resistencia por parte de los	**DA** 1. Inventariar y valorar los activos de la organización Contratar personal con conocimientos en el manejo del sistema SGSI	**Necesidad de seguridad** Actualmente la información de ARFUSOG, se encuentra vulnerable frente a	

empleados para implementar el Sistema SGSI	ataques cibernéticos y acceso a la información por parte de terceros ya que no cuenta con un sistema.

Nota. Elaboración propia

Síntesis de las Oportunidades de Mejora del SGSI con la Finalidad Hallar Posibles Soluciones.

Con el objetivo de profundizar en el diagnóstico de la matriz DOFA, se realizó un análisis mediante el desglose de los datos hallados inicialmente en la entrevista, la encuesta y el mapa de empatía, de esta manera se retomaron las debilidades, fortalezas, amenazas y oportunidades que tiene la empresa a nivel interno y externo, de tal manera que se tenga una mirada global del contexto de la seguridad de la información, la necesidad del diseño del sistema SGSI para ARFUSOG y los beneficios que tiene para la empresa disponer de un SGSI. De la misma manera se evidencio.

A nivel interno se identificó que la administración no tiene implementado una cultura organizacional basada en un sistema de seguridad de la información que permita tener disponibilidad, integridad y confidencialidad de la información para el uso de los usuarios internos y externos, orientados siempre hacia la mejora continua de procesos y el uso eficiente de recursos de la entidad.

A nivel externo se identificaron oportunidades y amenazas de la empresa frente a la competencia, con la finalidad de crear estrategias que le permitan estar a la vanguardia de la economía cambiante.

En cuanto al contexto de seguridad de la información ARFUSOG, ha implementado procedimientos de control en la seguridad de la Información, como correos institucionales, Software contable e implementación de la licencia del office. Sin embargo, a un tiene procesos susceptibles de mejora, puesto que no cumple con estándares que propone la norma técnica (ISO-27001), en su numeral enfoque basado en procesos. No obstante, ARFUSOG tiene la Necesidad de un diseño de seguridad de la información porque se encuentra vulnerable frente a

ataques cibernéticos y acceso a la información por parte de terceros ya que no cuenta con un sistema SGSI. Por otro lado, las debilidades del sistema de gestión de seguridad de información, nos permite determinar factores de vulnerabilidad o procedimientos deficiente en la ejecución del sistema de información de los documentos y archivo de la empresa.

Análisis de las Debilidades del Sistema de Gestión de Seguridad de la Información través de Herramientas de Gestión de Proyectos.

En esta etapa se determinará el análisis de las debilidades del sistema de seguridad de la información mediante las herramientas de gestión de proyecto diagrama de Pareto y espina de pescado descritas a continuación:

Análisis las Debilidades del SGSI; Mediante de la Espina de Pescado, Diagrama de Pareto y los 5 Porqués, para Generar Propuestas en la Optimización del Sistema

Herramienta Diagrama de Pareto

En la figura 2, llamada diagrama de Pareto se detectaron las principales causas por las cuales la asociación ARFUSOG, no ha llevado a cabo un Sistema de Gestión de Seguridad de la Información (SGSI), no obstante, se puede evidenciar que las 8 primeras causas identificadas son responsables del 80% de las dificultades que representan un riesgo para el sistema de información.

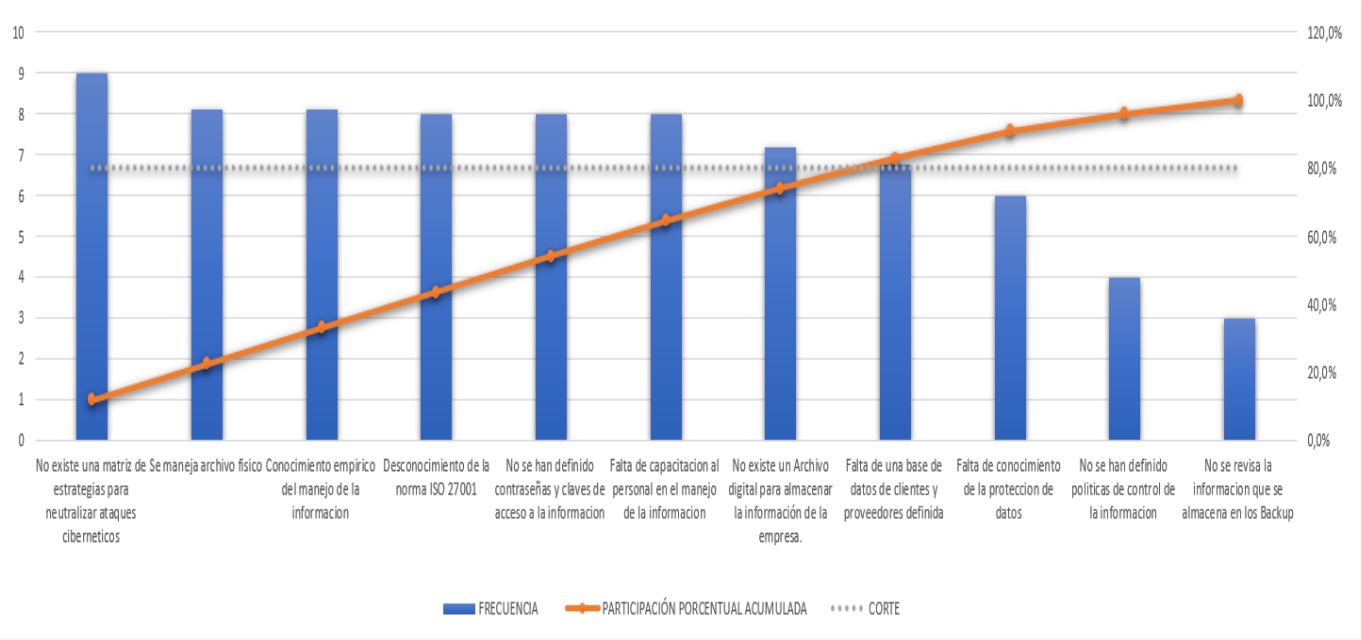
El diagrama de Pareto muestra que las tres causas restantes corresponden al 20% del problema, las cuales no representan un riesgo para la entidad, no afectan la seguridad de la información como la disponibilidad, confidencialidad e integridad de esta, sin embargo, se deben mantener monitoreadas e identificadas.

A través de la gráfica se pueden visualizar los riesgos que merecen ser atendidos con urgencia por parte de la empresa de manera que se puedan dirigir acciones para responder ante la

necesidad latente de proteger la información y reducir el impacto del riesgo al que están expuestos los activos y el nivel de criticidad para cada uno. Con la aplicación del diagrama de Pareto se determinaron las anomalías de la organización en cuanto al sistema de información; de esta manera se identificaron problemas graves que deben abordarse primero asignando un orden de prioridad para cada caso.

Figura 2

Diagrama de Pareto – Debilidades ARFUSOG



Nota. Elaboración propia

La tabla 4 denominada Herramienta de diagrama de Pareto, permitió identificar las fallas relevantes del sistema de seguridad de la información que tiene la entidad, en cuanto a la frecuencia con la que se presenta, la incidencia que tiene y el porcentaje con respecto a temas triviales o pocos vitales para la asociación como es la deficiencia de procedimientos, deterioro de documentos, perdida de información, escasez de un sistema que almacene la información, el personal de la

empresa no tiene contraseñas para acceder a los computadores y la carencia de una matriz de riesgos como herramienta de seguimiento de procesos.

En la tabla 4, se realiza una visión global de los problemas que dificultan el desarrollo del sistema de seguridad de la información al interior de la empresa, el diagrama de Pareto simplifica la clasificación de factores negativos según su peso o importancia dentro de un proceso; teniendo en cuenta esa clasificación, el 20% de factores más determinantes, permite que el 80% sea una consecuencia.

Tabla 4.

Herramienta de Diagrama de Pareto

DIAGRAMA DE PARETO								
Se ingresaron en la tabla la incidencia y la frecuencia reportada	**CÁLCULOS AUTOMÁTICOS - ORDEN DESCENDENTE**							
Incidencia	**Frecuencia**	**Ranking**	**Posición Real**	**Incidencia Ordenada**	**Frecuencia**	**Participación Porcentual**	**Participación Porcentual Acumulada**	**Corte**
Desconocimiento de la norma ISO 27001	8	4	1	No existe una matriz de estrategias para neutralizar ataques cibernéticos	9	12%	11,8%	80,0 %
Falta de conocimiento de la protección de datos	6	9	2	Se maneja archivo físico	8	11%	22,5%	80,0 %
No existe un Archivo digital para almacenar la información de la empresa.	7	7	3	Conocimiento empírico del manejo de la información	8	11%	33,1%	80,0 %

No se revisa la información que se almacena en los Backup	3	11	4	Desconocimiento de la norma ISO 27001	8	11%	43,6%	80,0 %
No se han definido políticas de control de la información	4	10	5	No se han definido contraseñas y claves de acceso a la información	8	11%	54,1%	80,0 %
No se han definido contraseñas y claves de acceso a la información	8	5	6	Falta de capacitación al personal en el manejo de la información	8	11%	64,6%	80,0 %
No existe una matriz de estrategias para neutralizar ataques cibernéticos	9	1	7	No existe un Archivo digital para almacenar la información de la empresa.	7	9%	74,1%	80,0 %
Se maneja archivo físico	8	2	8	Falta de una base de datos de clientes y	7	9%	82,9%	80,0 %

				proveedores definida				
Conocimiento empírico del manejo de la información	8	3	9	Falta de conocimiento de la protección de datos	6	8%	90,8%	80,0 %
Falta de capacitación al personal en el manejo de la información	8	6	10	No se han definido políticas de control de la información	4	5%	96,1%	80,0 %
Falta de una base de datos de clientes y proveedores definida	7	8	11	No se revisa la información que se almacena en los Backup	3	4%	100,0%	80,0 %
Total					**76**			

Nota. Elaboración propia

Asimismo, con las herramientas de Gestión de proyectos, diagrama de Pareto y la espina de pescado se realizó un análisis detallado de las causas probables del problema objeto de estudio, para plantear posibles soluciones al sistema de seguridad de la información. A continuación, encontrara el análisis realizado al diagnóstico mediante la herramienta de gestión de proyectos espina de pescado

Herramienta Espina de Pescado

A través de la herramienta espina de pescado, se realizó un análisis interno de las debilidades del sistema de seguridad de la información de la asociación ARFUSOG, donde se determinaron factores como diseño, personas, desarrollo, métodos y herramientas.

Para empezar en el primer factor nombrado como diseño no se precisaron controles de seguridad para el acceso, igualmente la empresa no tiene una base de clientes y proveedores definida; de la misma manera no cuenta con un sistema de datos estructurado, y además no existe un archivo digital para almacenar la información

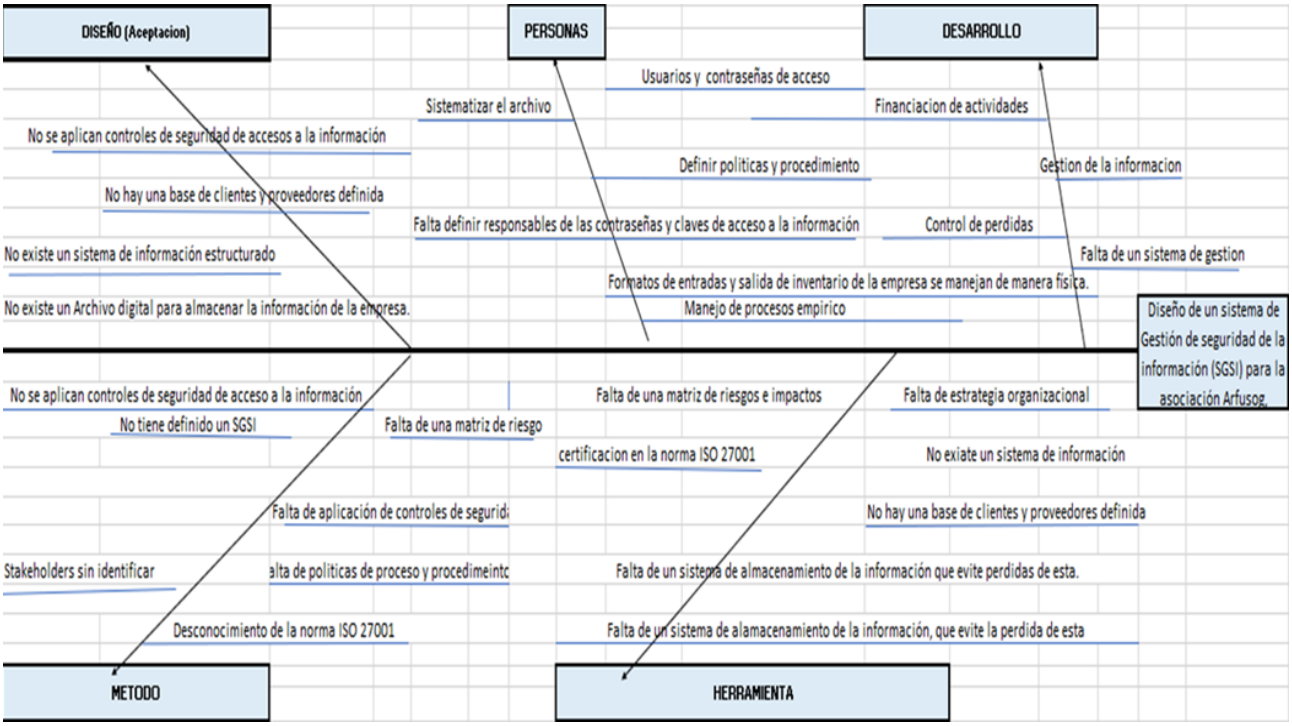
En el factor Personas, la entidad se carece de usuarios y contraseñas de acceso a la información; por otro lado, no tiene sistematizados los archivos; y no cuenta con políticas y procedimientos establecidos; en efecto no ha asignado responsables del sistema; sin restar importancia al manejo de procesos de forma empírica. Ahora bien, en el factor Desarrollo, se evidencia la carencia de financiación de actividades en pro de la seguridad de la información, en efecto no existe un control de pérdidas de información, además, formatos de entradas y salidas de inventario de la empresa se manejan en físico. Cabe señalar que en el factor Método, se halló ausencia de controles para acceder a la información; también se identificó que la empresa no tiene definido un sistema SGSI, y se encontró deficiencia en la identificación de los

Stakeholders; cabe resaltar que el personal administrativo y operativo desconocen la norma técnica (ISO-27001), tal como se indica el numeral 02 enfoque basado en procesos. (NQA, 2013)

Por consiguiente, en el factor Herramienta, queda detallado la inexistencia de la matriz de riesgos e impactos; en ese sentido ARFUSOG no tiene estrategias organizacionales enfocadas en el sistema de datos, conviene mencionar que la empresa carece un sistema capaz de almacenar la información para evitar pérdidas. La figura 3, diagrama espina de pescado se realizó el desarrollo del diagnóstico de la empresa como análisis tanto interno como externo, para comprender cuáles son las características específicas de las causas y efectos del problema objeto de estudio.

Figura 3

Análisis de las Debilidades Encontradas a través de la Espina de Pescado



Nota. Elaboración propia

Herramienta de Análisis los 5 Porqués

Mediante la aplicación de la herramienta de los 5 porqués, se pudo determinar que ARFUSOG, requiere del diseño de procedimientos que sirvan de guía para el desarrollo de procesos como, controles, políticas y capacitación al personal para el manejo de la información de tal manera que se puedan identificar y mitigar los riesgos que se exponen en cada activo de información de la empresa y que pueden afectar procesos de la organización, de la misma manera se identificó que la empresa no cuenta con la creación de una matriz de asignación de permisos y contraseñas por área a cada usuario de tal manera que indique que usuarios tienen permisos para visualizar, modificar y eliminar archivos, esto con el objetivo de mantener la disponibilidad, integridad y confidencialidad de la información. En la tabla 5 herramienta de análisis de los 5 porques, se realizó el cuestionamiento sistemático a los problemas identificados del sistema SGSI de la empresa ARFUSOG, donde se encontró la causa raíz de las dificultades más relevantes y precisos de la organización, cabe resaltar que para cada una de las causas se encontraron entre tres y cinco motivos que la generaron.

Con la aplicación de la herramienta de los 5 porqués, se encontró que la entidad carece de la implementación de políticas aplicadas al sistema de información, debido al desconocimiento de la norma técnica para el diseño del SGSI. Además, se detectó la inexistencia de un sistema de almacenamiento de la información, por ende, la cusa raíz identificada fue la falta de capacitación al personal en el manejo del archivo, de la misma manera cada empleado guarda la información en memorias USB, corriendo el riesgo de pérdida de datos y virus que pueden acceder al PC y que se puede dañar archivos e información relevante de la empresa. Por ende, se identificó que la causa raíz encontrada es la falta de creación de un comité de seguridad de la información que se encargue de realizar controles al sistema de información para la mejora continua de los procesos.

Tabla 5

Herramienta de los 5 Porqués

Análisis causa raíz – Cinco Porqués						
Causa - Espina de pescado	**Porque #1**	**Porque # 2**	**Porque #3**	**Porque #4**	**Porque #5**	**Causa raíz – identificada**
Falta de políticas de procesos y procedimientos	Porque, no se han diseñado y estructurado para para que haya una mejora continua en los procedimientos de la empresa	Porque, no se evidencia políticas, que documenten los procesos de la empresa	Porque, la empresa no proporciona una hoja de ruta para las operaciones diarias de la esta.	Porque, no hay reglas que orienten al comportamiento para cada situación que se presente en la empresa.	N/A	Porque, no se han diseñado y estructurado, una hoja de ruta para la operación diaria, ni normas que oriente al comportamiento para cada situación
Desconocimiento de la norma ISO-27001	Porque, los empleados de la empresa no tienen conocimiento de la norma	Porque, no se ha capacitados a los empleados sobre la norma				Porque, no se ha capacitado sobre la importancia de aplicar la norma para mejora continua de los procesos de la empresa
No existe un Archivo digital para almacenar la información de la empresa.	Porque, no se tiene orden y control del archivo de la empresa	Porque, se maneja los archivos físicos	Porque, el personal maneja el archivo de la información de forma empírica	Falta de capacitación al personal		Descornamiento del manejo del archivo
No existe un sistema de información estructurado	Porque, no se tiene conocimiento de la norma ISO-27001.	Porque, la empresa no está certificado en normas de				Porque, no se tiene conocimiento de la importancia de normas

		protección y custodio de documento.		ISO- 27001 para los procesos de la empresa.
No se aplican controles de seguridad de accesos a la información	Porque, no está establecido quien es el responsable del manejo de la información	Porque, no hay un área de soportes técnica para el manejo de la información	Porque, no existen controles de seguridad para el almacenamiento de la información.	No hay un responsable destinado para el control de la información de la empresa
Falta de un sistema de almacenamiento de la información que evite perdidas de esta.	Porque, no se ha estructurado un sistema de respaldo de la información de la empresa	Porque, no se tiene un matriz donde se evidencia la información que contiene cada uno del archivo y el acceso a esta.	Porque, no están debidamente rotulados los archivo	Falta de un sistema gestión de seguridad de información que respalde el contenido de los archivos.
Falta definir responsables de las contraseñas y claves de acceso a la información	Porque, no se ha definido el responsable	Porque, la empresa desconoce el manejo el manejo de un sistema de gestión de seguridad de la información		Porque, la empresa desconoce el daño que terceros pueden ocasionar a la información si no se tiene un control y permisos establecidos.
Falta de una matriz de riesgos e impactos	Porque, no se tiene una base de dato con su archivo seleccionado.	Porque no hay procesos estructurados y automatizad		Porque, la empresa no a delegado a una persona que se dedique hacer controles y

		os en la empresa	seguimiento a los procesos.
No hay una base de clientes y proveedores definida	Porque, el archivo que se maneja es físico y no está debidamente documentado		Porque la persona encargada de la información es empírica
Formatos de entradas y salida de inventario de la empresa se manejan de manera física.	Porque, porque no está sistematizado el proceso de entrada y salida de inventario.	Porque la empresa no cuenta con una estrategia organizacional que imponga la filosofía de los procesos y procedimiento	Porque no sean definido funciones y responsable para el manejo de un sistema de gestación de seguridad de la información

Nota. Elaboración propia. Fuente. Formato del cuadro por Ana María Gómez (2018), del trabajo de grado Mejoramiento de producción y ventas de la empresa confecciones Luthier; obtenido de: https://core.ac.uk/download/pdf/232126645.pd

Análisis Alternativas de Solución Mediante la Herramienta Lluvia de Ideas

La tabla 6, herramienta lluvia de ideas tiene como punto de partida las causas identificadas en la espina de pescado, se evidencia la carencia de un sistema integrado de seguridad de la información; resulta entonces importante mencionar que esta herramienta apunta a las raíces de las causas, que posteriormente da paso a pensar en ideas para eliminar las raíces de esas causas identificadas.

Por consiguiente, se abordarán puntualmente el principio de las causas, entendiendo que en la herramienta espina de pescado se trataron las causas generales por las cuales ARFUSOG, no cuenta con un SGSI, de igual forma no existe un comité encargado crear políticas y controles al sistema de seguridad de la información, en consecuencia los empleados no son capacitados en la norma técnica (ISO-27001), tal como se indica el numeral 02 enfoque basado en procesos. (NQA, 2013)

Además, no están definidos los controles que inician procesos de automatización de documentos y compra de dispositivos para almacenar la información, la empresa tampoco ha definido un área responsable del sistema de seguridad de la información y que a su vez realice soportes técnicos, en concreto la organización se desconoce los procesos para establecer un sistema de información de forma segura, no se dan procesos estructurados y automatizados.

Con base, en dicho anteriormente surgen ideas que buscan apuntar a eliminar dichas causalidades que se convierten en impedimentos para el manejo correcto de la información, es indispensable definir el alcance y contar con un comité de seguridad de la información; capacitar a los empleados del área administrativa y operativa en la norma técnica; adquirir un dispositivo de almacenamiento conectado a una red que recupere datos en un punto centralizado; definir activos que tiene la empresa y de acuerdo con ello aplicar controles como contraseñas de

acceso a la información, definir responsables para que protejan la información para mantener la disponibilidad; confidencialidad e integridad; y en definitiva diseñar una matriz de riesgos para seguimiento control y monitoreo de la información.

Tabla 6

Análisis del problema SGSI Encontrado en la Espina de Pescado, Mediante la Herramienta Lluvia de Ideas

Análisis causa raíz – Mediante la lluvia de ideas		
Causa - Espina de pescado	**Causa raíz identificada**	**Ideas para eliminar la causa raíz identificada**
Falta de políticas de procesos y procedimientos	Falta definir un comité que se encargue de las políticas y controles para el sistema de Seguridad de la información	Definir el alcance y el comité del SGSI de acuerdo con la norma ISO-27001 y los objetivos de la organización
Desconocimiento de la norma ISO-27001	Falta de capacitación al personal sobre la norma técnica de Seguridad de la información	Implementar capacitaciones para el personal del área administrativa y operativa
No existe un Archivo digital para almacenar la información de la empresa.	Falta de definir controles que den inicio al proceso de automatización de documentos y compra de un dispositivo que almacene la información	Adquirir un dispositivo (NAS) que permita el almacenamiento de la información
No se aplican controles de seguridad de accesos a la información	La entidad no ha definido un área responsable del sistema SGSI y de soportes técnicos	Definir los activos de información que tiene la empresa y de acuerdo con ello aplicar los controles como contraseñas de acceso a la información
Falta definir responsables de las contraseñas y claves de acceso a la información	La empresa desconoce el manejo el manejo de un sistema de gestión de seguridad de la información	Definir el área que será la responsable de salvaguardar la información y mantenerla disponibilidad, confidencialidad e integridad de esta

Falta de una matriz de riesgos e impactos	No existen procesos estructurados y automatizados en la empresa en cuanto al sistema de seguridad de la información	Diseñar una matriz de riesgos que permita el seguimiento, control y monitoreo para la mejora continua

Nota. Elaboración propia

Síntesis de las Herramientas Aplicadas al Sistema SGSI

En el desarrollo de la fase de análisis del diagnóstico se aplicaron las siguientes herramientas de gestión de proyectos como son, diagrama de Pareto, espina de pescado, los 5 porqués, lluvia de ideas, juicio de expertos, y matriz de priorización de causas, las cuales permitieron determinar el diagnostico SGSI a través de resultados obtenidos por cada una de las herramientas fueron los siguientes:

El diagrama de Pareto arrojo que el 80 % de los problemas se derivan del 20 % de las causas, es decir que el 80% de los problemas son poco triviales en la empresa ARFUSOG y se generan por la aplicación del conocimiento empírico del manejo de la información; desconocimiento de la Norma técnica ISO-27001; falta de capacitación al personal en el manejo de la información, no existe una base de datos digital de los clientes y proveedores; carece contraseñas y claves de accesos a la información y el 20% de las causas que corresponde a muchos vitales los cuales se dan por la falta de protección de datos; no se han definido las políticas de seguridad de la información; la empresa no revisa la información que se almacena en los Backup.

Es oportuno resaltar que con la herramienta espina de pescado, los resultados encontrados fueron los siguientes: ARFUSOG, no cuenta con un sistema de archivo digital; el Sistema de información carece de la definición de usuarios y contraseñas; ausencia de un sistema de Seguridad de la Información; la inexistencia de responsables de la seguridad de la

información; no tienen un sistema de almacenamiento en red para que los usuarios accedan a la información.

En cuanto a la herramienta de los 5 porqués, se encontró como resultado la causa raíz de las dificultades más relevantes del sistema SGSI de la empresa ARFUSOG es falta de un diseño de procedimientos que sirvan de guía para el desarrollo de procesos de seguridad de la información como el diseño de controles, establecer políticas, identificación de riesgos e impactos, definir activos de la seguridad de la información y capacitación al personal de la empresa en manejo de la seguridad de la información y el archivo digital.

Conviene precisar que a través de la herramienta lluvia de ideas se encontró como resultado las raíces de las causas principales del problema SGSI de ARFUSOG, como es la carencia de un comité que se encargue de definir el alcance del sistema SGSI y responsables para que protejan la información y mantenerla disponibilidad; confidencialidad e integridad de esta; y en definitiva la inexistencia de una matriz de riesgos para seguimiento control y monitoreo de la información.

Valoración de Alternativas de Solución

Estimación de Posibles Soluciones SGSI a través del uso de Herramientas de Gestión de Proyectos

En esta etapa se determinarán las posibles soluciones del sistema de seguridad de la información mediante el uso de las herramientas de gestión de proyectos como matriz de priorización Juicio de expertos y Criterio de decisión de la norma ISO-27001. A continuación, se describen los resultados que arrojaron las alternativas de solución aplicadas al SGSI de la empresa ARFUSOG.

Determinación de la Mejor Solución según el Sistema de Información

Alternativa de Solución 1 - Matriz Priorización:

A través de la herramienta Matriz de priorización se puedo evaluar de manera clara y precisa las causas del problema del sistema SGSI que se presenta en la empresa ARFUSOG. De esta manera se identificaron problemas claves a evaluar, para ello se definen criterios de ponderación determinando un nivel de importancia a cada uno de ellos con el fin de asignarle una puntuación a los problemas o variables identificadas con la finalidad que la empresa tome una decisión e implemente alternativas de solución.

A continuación, se relaciona la matriz de priorización de causas en la tabla 10, que es una herramienta de gestión y control de proyectos, la cual se utilizó para validar la información de la espina de pescado y el diagrama de Pareto. Esta herramienta consiste en elaborar una tabla en la que se presentan diferentes criterios que permiten asignar un porcentaje o valor a cada problema, que va desde el 0% hasta el 100% de la ponderación de esta manera se prioriza las causas principales del problema y permite que la empresa tome una decisión e implemente alternativas de solución. Con la matriz de prioridad se pudo validar y reafirmar que la empresa debe

implementar una serie de procesos que conllevan a la mejorar el sistema de seguridad de la información.

A continuación, encontrara la tabla 7 matriz de priorización de causas.

Tabla 7

Matriz de Priorización de Causas Aplicado a las Herramientas Espina de Pescado y Diagrama de Pareto

Matriz de Priorización de Causas, Espina de Pescado y diagrama de Pareto									
Ingrese las puntuaciones en la tabla a continuación. Utilice los números enteros del cero al cinco (del 0 al 5) para calcular la puntuación de priorización de requisitos	**Criterio Peso Los valores de peso total deben ser iguales a 100.**								**Peso Total (100)**
	12,5	**12,5**	**12,5**	**12,5**	**12,5**	**12,5**	**12,5**	**12,5**	**100**
Causas que se repiten en la espina de pescado y el	**Valor para el negocio**	**Riesgo del negocio**	**Desafíos de implementación**	**Posibilidades de éxito**	**Conformidad**	**Relación con los requisitos**	**Urgencia**	**Acuerdo con las partes interesadas**	**Total Puntuación**

diagrama de Pareto									
Desconocimiento de la norma ISO-27001	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	**100**
No existe un Archivo digital para almacenar la información de la empresa.	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	**100**
No existe un sistema de información estructurado	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	**100**
Falta de un sistema de almacenamiento de la información que evite perdidas de esta.	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	**100**

Falta definir responsables de las contraseñas y claves de acceso a la información	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	**100**
Falta de una matriz de riesgos e impactos	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	**100**
La empresa no tiene una base de clientes y proveedores definida	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	**100**
Formatos de entradas y salida de inventario de la empresa se manejan de manera física.	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	**100**

Nota. Elaboración propia

Alternativa de Solución 2 - Juicio de Expertos

Se aplica la herramienta de Juicio de expertos para validar la confiabilidad de las herramientas de gestión de proyectos espina de pescado y diagrama de Pareto, de acuerdo con el análisis realizado se puede decir que las dos herramientas son de suma importancia para identificar las causas de la problemática de investigación para darle solución al problema de disponibilidad, integridad y confidencialidad de la información de la empresa ARFUSOG, y a su vez evitar la pérdida y deterioro de datos por la inexistencia del SGSI, para la Asociación ARFUSOG, el experto sugiere la eliminación de aspectos innecesarios y añade procesos innovadores que agregan valor a los procedimientos de la organización, como parte del proceso de rigurosidad metodológica brinda confiabilidad a los contenidos del problema identificado.

Teniendo en cuenta la valoración de los expertos en la tabla 8, Se puede evidenciar que las herramientas de gestión de proyectos aplicadas en esta investigación determinaron las principales causas del sistema de seguridad de la información de la empresa ARFUSOG, facilito la identificación de las debilidades y fortalezas de la entidad permitiendo establecer criterios y pautas para estructurar el diseño del Sistema SGSI.

Tabla 8

Aplicación del Juicio de Expertos para Validar las Herramientas de Espina de Pescado y Diagrama de Pareto

Juicio De Expertos Para Validar Las Herramientas Aplicadas						
		Valoración				
Aspectos por evaluar	**Criterio del experto**	**1 Muy malo**	**2 Malo**	**3 Regular**	**4 Bueno**	**5 Muy Bueno**
1.Desconocimiento de la norma ISO 27001	Establecer políticas, metas, procesos y procedimientos de seguridad pertinentes para gestionar riesgos y mejorar la seguridad de la información, con Entregar resultados basados en políticas y resultados. objetivos generales de la organización		X			
2.Falta de conocimiento de la protección de datos	Contratar una persona que tenga conocimiento en manejo de protección de la información y los datos, general espacio de capacitación al personal de la empresa en manejo de datos.	X				
3.No existe un Archivo digital para almacenar la información de la empresa.	Emprender acciones que permitan la sistematización de todos los documentos y la información de la empresa.	X				

4.No se revisa la información que se almacena en los Backup	Capacitación al personal, en la preservación de la confidencialidad, la integridad y la disponibilidad de la información.	X	
5. No se han definido políticas de control de la información	Implementar políticas basadas en un enfoque hacia la mitigación de riesgo con la finalidad de establecer estrategia y mejorar la seguridad de la información.		X
6. No se han definido contraseñas y claves de acceso a la información	Definir políticas de control de acceso a la información del personal interno y de terceros.		X
7. No existe una matriz de estrategias para neutralizar ataques cibernéticos	Definir el alcance y límites del SGSI en término de las características de la organización su ubicación sus activos, la tecnología e implementar software y limitar el acceso a los usuarios con claves y contraseña.		X
8.Falta de capacitación al personal en el manejo de la información	Definir los responsables de la seguridad de la información en cuanto a la confidencialidad, integridad y disponibilidad de esta.		X
9.Falta de Conocimiento	Crear, sistematizar la información e implementar	X	

empírico del manejo de la información	controles que disminuyan falla del manejo de la información		
10.Falta de un sistema de almacenamiento de la información que evite perdidas de esta.	Capacitar al personal en cuanto al manejo de la información para evitar riesgo en perdida, deterioro y daño de la información		X
11.Falta de una base de datos de clientes y proveedores definida	Determinar la base de dato de cliente y proveedores de la empresa para evitar perdida del contacto y los inventarios se suministran		X
	Total	**4**	**7**

Nota. Elaboración propia

Alternativa de Solución 3 - Criterio de Decisión

la norma técnica ISO-27001, está integrada por las buenas prácticas del sistema de seguridad de la información que se basa en proteger la confidencialidad, integridad y disponibilidad de la información de un sistema SGSI, para ello es importante la aplicación de varias fases del proceso como son; establecer los requisitos y controles de mejora del SGSI; definir la política de seguridad de la organización; definir el alcance del Sistema de Gestión de Seguridad de la Información; definir la gestión del riesgo; análisis de riesgos en activos de información como amenazas y vulnerabilidades; selección de controles para usuarios internos y externos; revisión del Sistema de Gestión de Seguridad de la Información y de sus medidas preventivas y correctivas.

Utilización de la Norma Técnica ISO-27001, en su Numeral 2 literal a; Enfoque Basado en Procesos

Con la finalidad de establecer requisitos y controles de mejora del SGSI para la empresa asociación ARFUSOG, se tomará como punto de partida de la Norma técnica (ISO-27001), el numeral 02 Enfoque Basado en Procesos; permite que los directivos de la entidad se enfoquen principalmente en los siguientes aspectos:

En primera instancia se encarga de comprender los requisitos de seguridad de la información de la empresa, y la necesidad de establecer la política y objetivos en relación con la seguridad de la información. (ICONTEC, 2006,p.6)

El segundo momento se basa en implementar y operar controles para manejar los riesgos de seguridad de la información de una organización en el contexto de los riesgos globales. (ICONTEC, 2006,p.6)

Como tercero la norma ISO-27001), señala que "promueve la adopción de un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el SGSI de una organización". (ICONTEC, 2006,p.6)

Para la asociación ARFUSOG, establecer los requisitos para la seguridad de la información es de vital importancia puesto que le permitirá a la empresa tener controles para la protección de datos, la disponibilidad y la integridad de esta, con la finalidad de establecer una ruta para el diseño del SGSI.

Cabe resaltar que el alcance del proyecto se limita solo a establecer los requisitos y controles del sistema de Seguridad de la Información para la empresa asociación ARFUSOG, de la ciudad de Sogamoso, mediante la utilización de una metodología compuesta por fases, etapas

y actividades (Ver figura 5, llamada metodología utilizada para el desarrollo del sistema SGSI de ARFUSOG).

Es importante mencionar que esta propuesta debe ser aprobada por la gerencia de tal manera que la empresa pueda definir los recursos necesarios para la operación, mantenimiento y mejora del sistema de información. Un Sistema SGSI tiene muchas ventajas para contrarrestar el riesgo cibernético, es cada vez más importante contar con un sistema de gestión de seguridad de la información basado en el estándar (ISO-27001), para proteger los datos y prevenir la exposición de datos por parte de usuarios internos y externos.

Definición de los Activos para Proteger en el Sistema de Información SGSI

La identificación de los activos de información se determinó de acuerdo con el alcance definido para el SGSI de ARFUSOG, para el área de seguridad de la información; se tuvo en cuenta el grado de criticidad y el nivel de protección de los activos, se diseñó una tabla donde se indica el tipo de activo y su denominación. Cabe resaltar que la entidad no tiene definido un inventario de sus activos, se realizaron reuniones con la ingeniera Patricia de la empresa para recopilar la información.

A continuación, en la tabla 9 se relacionan los activos de información de la entidad como son, Disponibilidad de la información (DI); Integridad de datos (IN); Confidencialidad de la información (CI) y criterios de valoración de los activos de información, tales como, Muy bajo (0-1); Bajo (2-3); Medio (4-5-6); Alto (7-8); Muy alto (9); Emergencia (10)

Tabla 9

Activos del Sistema de Seguridad de la Información y su Nivel de Riesgo

Activos y nivel de riesgos y perdida de la Información					
Tipo de activo /Sigla	**Descripción general**	**Cantidad**	**Tipo de valoración**	**Riesgo**	**puntuación del valor**
	Módulo contable	1	DI y IN	Bajo	3
Software (SF)	Módulo Comercial	1	DI y IN	Bajo	3
	Módulo de inventario	1	DI y IN	Bajo	3
	Proveedores	1	CI	Alto	8
	Clientes	1	CI	Alto	8
Base de datos/ Información	Sistema de redes de recolección de información	7	CI	Alto	8
(BI)	Memorias USB	2	DI y IN	Muy alto	9
	Documentos varios (Archivo físico)	1	DI-IN-CI	Muy alto	9
	Contratos	9	CI	Alto	8
	Correo electrónico	1	DI y IN	Alto	8
	Plataformas para reuniones virtuales	1	DI y IN	Bajo	3
Servicios y	Líneas telefónicas	1	DI	Bajo	3
Personas (SP)	Actualizaciones de hosting	1	DI y IN	Bajo	3
	Personal colaborador de procesos	9	DI-IN-CI	Muy Alto	9

Equipos informáticos (EI)	Computadores	1	DI y IN	Muy alto	9
	Scanner	1	DI y IN	Alto	8

Nota. Elaboración propia

Cada nivel de riesgo requiere algún tipo de control por parte de la entidad, ya sea de tipo preventivo el cual se encarga de pronosticar la probabilidad de ocurrencia y del impacto que conlleva en la implementación de la estrategia de tal forma que sea controlado, monitoreado y evaluado de manera permanente; y controles correctivos que permiten a la administración tomar decisiones para prevenir hechos que puedan afectar los objetivos misionales de la entidad. Para la valoración de los activos de información se tuvieron en cuenta los siguientes valores:

Emergencia (10). Es un riesgo que puede afectar la estrategia corporativa, esta seda de manera repentina o se deriva de un riesgo conocido.

Muy Alto ((9). Es un riesgo que afecta todas las actividades la empresa convirtiéndola en vulnerable ante ciertas situaciones, dicho riesgo debe ser controlado, monitoreado y evaluado de manera permanente.

Alto (7-8). Un riesgo alto es aquel que afecta de manera significativa las operaciones de la entidad debe ser controlado, monitoreado y evaluado de manera permanente.

Medio (4-5-6). Riesgo que puede provenir de factores internos o externos que pueden afectas las operaciones de la empresa y por ello deben definir controles claves que los minimicen.

Bajo (2-3). Son los riesgos permanentes que se presentan cada día en la realización de las diferentes actividades que si no son monitoreados pueden subir su nivel de vulneración a las actividades de la empresa.

Muy bajo (0-1): Son riesgos que se dan por el día a día de la empresa y que al igual que los otros deben ser monitoreados para que no afecten en el futuro a la entidad.

La asociación ARFUSOG, cuenta con información de tipo privada, la cual se maneja entre las diferentes áreas de la organización tales como; Información de tipo interna como carpetas compartidas, documentos que circulan al interior de la organización entre las diferentes áreas, Información de tipo pública que es la información a la cual tienen accesos los usuarios externos como páginas web. Las amenazas identificadas para los activos de seguridad de información son:

Medio ambiente. consiste en la falta de mantenimiento de equipos, los cuales se llenan de polvo y con el paso del tiempo se deterioran; alteración de equipos por carga de energía eléctrica esto se da por no contar con un sistema de alimentación interrumpida (UPS); equipos ubicados en lugares que tienen humedades que pueda causar fallas eléctricas etc.

Manipulación del software. vulneración del sistema por parte de personas no autorizadas; equipos mal configurados; virus que afectan el sistema operativo de equipos; uso de páginas maliciosas y equipos sin contraseñas ni usuarios.

Saturación del sistema. inexistencia de servidores que procesen la información y la distribuyan a los equipos conectados; almacenamiento excesivo de archivos que colocan lento el sistema y correos sin licencia.

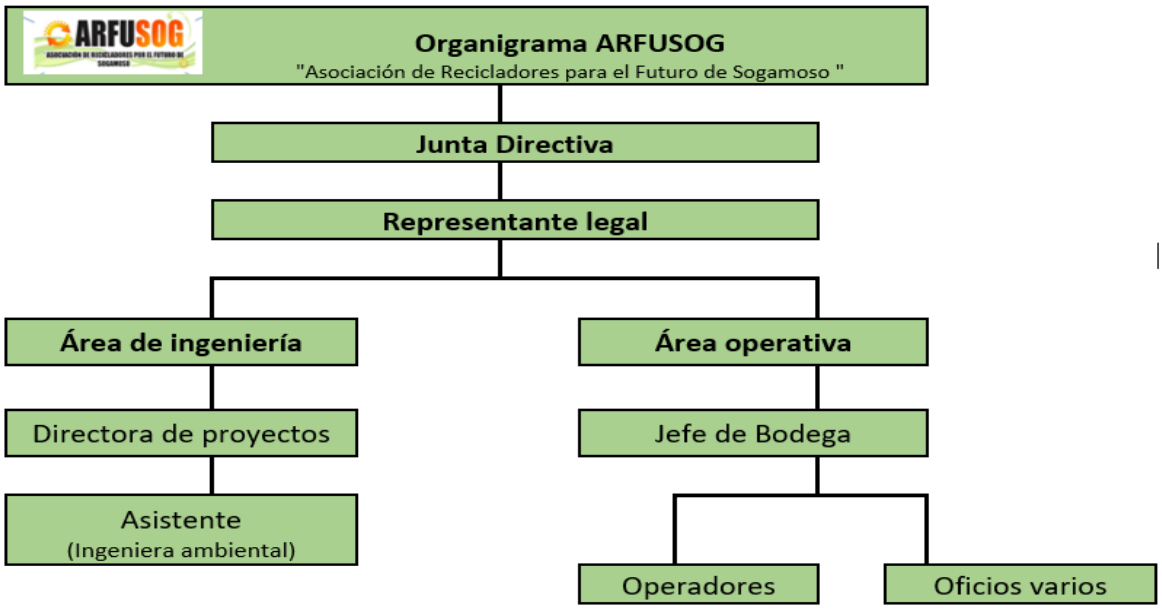
Corrupción de datos. No existen controles de acceso para ingresar a las bases de datos; suplantación de usuarios para el ingreso al sistema, fallas del sistema de seguridad de la información; hurto de equipos; exempleados con contraseñas activas; ataques cibernéticos por parte de terceros y falta de cambio de contraseña de manera periódica,

Definición los Responsables de la Seguridad de la Información para ARFUSOG

La asociación ARFUSOG, no tiene una persona encargada del manejo de la seguridad de la información, cada empleado es responsable de hacer las copias de seguridad, estos a su vez manejan memorias USB para el almacenamiento de la información las cuales son vulnerables a daños, virus y perdida de la información.

A continuación, se relaciona el organigrama de la empresa ARFUSOG, el cual fue creado de acuerdo con la información facilitada por la ingeniera Patricia, con la finalidad de explicar cómo están divididos en departamentos de la empresa y colaboradores:

Figura 4



Organigrama de ARFUSOG

*Nota***.** ARFUSOG (2022); información facilitada por la ingeniera ambiental

De acuerdo con el organigrama se recomienda que la seguridad de la información se asigne al departamento de Ingeniería bajo el cargo de la directora de proyectos, cabe resaltar que la seguridad de la información debe ser transversal a todas las áreas de la empresa.

Antes mencionado se sugiere que el área de ingeniería contrate un tecnólogo o ingeniero de sistemas que se dedique a la actualización, mantenimiento de equipos y acceso de contraseñas, o contratar con un tercero el proceso de supervisión y monitoreo permanente del sistema.

El área de ingeniería tendrá a cargo las siguientes responsabilidades las cuales son: primeramente, capacitar a lideres y colaboradores sobre procedimientos y políticas para el uso de la seguridad de la información; Seguidamente monitorear y controlar todas las acciones que coloquen en riesgo la seguridad de la información y como tercero implementar controles de seguridad de la información para tener certeza de la disponibilidad, confidencialidad e integridad de esta; de tal manera que se pueda determinar estrategias de mejora continua del SGSI y principalmente brindar soportes a usuarios de tal forma que el responsable pueda autorizar o restringir a usuarios el acceso a la información según su rol y responsabilidad dentro de la entidad.

Como cuarto punto, los usuarios internos de ARFUSOG deben diligenciar el formulario de política de confidencialidad y conflicto de intereses; reportar incidentes de seguridad y el mal uso de recursos. Por otro lado, el usuario de la información debe utilizar solo el software que haya adquirido de manera legal y con su respectiva licencia la organización. Cada jefe de área será quien indique el acceso y permiso para cada uno de sus colaboradores.

Establecimiento de las Políticas de Seguridad de la Información para la Empresa ARFUSOG

El coordinador de la seguridad de la información tiene la responsabilidad de implementar políticas y controles para monitorear de manera permanente el sistema de seguridad de la información de la empresa en busca de la mejora continua. En la tabla 10 se relacionan requisitos

generales que corresponden a las políticas de seguridad de la información, según la norma técnica (ISO-27001), en el numeral 02 enfoque basado en procesos.

Tabla 10

Políticas de Seguridad de la Información

ARFUSOG ASOCIACIÓN DE RECICLADORES POR EL FUTURO DE SOGAMOSO	**Políticas de Seguridad de la Información**	Versión 1. 22-10-2022
Objetivo	Establecer las políticas de seguridad de la información con la finalidad de implementar controles que protejan los activos de información y que esta pueda estar disponible, confiable e integra para los usuarios internos y externos de la organización.	
Alcance	Determinar las políticas de la seguridad de la información, el seguimiento y revisión del SGSI para la empresa asociación ARFUSOG	

Políticas generales

ARFUSOG, establece las siguientes políticas generales de seguridad de la información para la asociación.

Crear un comité de seguridad de información, encargado del mantenimiento, mejora y revisión permanente del sistema de seguridad de información.

Identificar los activos de información

Definir los controles a establecer para proteger la información

Definir fechas de auditorías al sistema de información

El sistema SGSI debe estar aprobado por la dirección de ARFUSOG

Políticas generales del Sistema de Seguridad de la Información de acuerdo con la Norma Técnica ISO – 27001

Con el objeto de revisar y hacer seguimiento permanente al sistema de seguridad de la información se especifican las siguientes políticas de manera general de acuerdo con la norma (ISO-27001):

Definir el alcance y límites del SGSI en términos de las características del negocio, la organización, su ubicación, sus activos, tecnología, e incluir los detalles y justificación de cualquier exclusión del alcance. (ICONTEC, 2006,p.12)

Definir una política de SGSI

En términos de las características del negocio, la organización, su ubicación, sus activos y tecnología, que: (ICONTEC, 2006,p.12)

Tenga en cuenta los requisitos del negocio, los legales o reglamentarios, y las obligaciones de seguridad contractuales. (ICONTEC, 2006,p.12)

esté alineada con el contexto organizacional estratégico de gestión del riesgo en el cual tendrá lugar el establecimiento y mantenimiento del SGS. (ICONTEC, 2006,p.12)

Aprobación del sistema por parte de la dirección. (ICONTEC, 2006,p.12)

Definir el enfoque organizacional para la valoración del riesgo.

Identificar una metodología de valoración del riesgo que sea adecuada al SGSI y a los requisitos reglamentarios, legales y de seguridad de la información del negocio, identificados. (ICONTEC, 2006,p.12)

Identificar los riesgos

identificar los activos dentro del alcance del SGSI y los propietarios2 de estos activos. (ICONTEC, 2006,p.12)

identificar las amenazas a estos activos. (ICONTEC, 2006,p.12)

identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas. (ICONTEC, 2006,p.12)

Identificar los impactos que la pérdida de confidencialidad, integridad y disponibilidad puede tener sobre estos activos. (ICONTEC, 2006,p.12)

Analizar y evaluar los riesgos

Valorar el impacto de negocios que podría causar una falla en la seguridad, sobre la organización, teniendo en cuenta las consecuencias de la pérdida de confidencialidad, integridad o disponibilidad de los activos (ICONTEC, 2006,p.13)

Estimar los niveles de los riesgos. (ICONTEC, 2006,p.13)

Implementación y operación del SGSI, de acuerdo con la norma técnica ISO-27001

De acuerdo con la norma técnica ISO-27001 la organización debe:

Formular un plan para el tratamiento de riesgos que identifique la acción de gestión apropiada, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información. (ICONTEC, 2006,p.15)

Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados, que incluye considerar la financiación y la asignación de funciones y responsabilidades. (ICONTEC, 2006,p.15)

implementar programas de formación y de toma de conciencia. (ICONTEC, 2006,p.15)

Gestionar la operación del SGSI. (ICONTEC, 2006,p.15)

Gestionar los recursos del SGSI. (ICONTEC, 2006,p.15)

Seguimiento y revisión del SGS, de acuerdo con la norma técnica ISO-27001

De acuerdo con la norma técnica ISO-27001 la organización debe:

Ejecutar procedimientos de seguimiento y revisión y otros controles para:

Detectar rápidamente errores en los resultados del procesamiento. (ICONTEC, 2006,p.15)

Identificar con prontitud los incidentes e intentos de violación a la seguridad, tanto los que tuvieron éxito como los que fracasaron. (ICONTEC, 2006, p.15)

Ayudar a detectar eventos de seguridad, y de esta manera impedir incidentes de seguridad mediante el uso de indicadores. (ICONTEC, 2006,p.15)

Determinar si las acciones tomadas para solucionar un problema de violación a la seguridad fueron eficaces. (ICONTEC, 2006,p.15)

Emprender revisiones regulares de la eficacia del SGSI (que incluyen el cumplimiento de la política y objetivos del SGSI, y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorias de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas. (ICONTEC, 2006,p.15

Medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad. (ICONTEC, 2006,p.15)

Revisar las valoraciones de los riesgos a intervalos planificados, y revisar el nivel de riesgo residual y riesgo aceptable identificado, teniendo en cuenta los cambios en:

La organización. (ICONTEC, 2006,p.15)

La tecnología. (ICONTEC, 2006,p.15)

Los objetivos y procesos del negocio. (ICONTEC, 2006,p.15)

Las amenazas identificadas. (ICONTEC, 2006,p.15)

La eficacia de los controles implementados. (ICONTEC, 2006,p.15)

Eventos externos, tales como cambios en el entorno legal o reglamentario, en las obligaciones contractuales, y en el clima social. (ICONTEC, 2006,p.15)

Realizar auditorías internas del SGSI a intervalos planificados. (ICONTEC, 2006,p.15)

Emprender una revisión del SGSI, realizada por la dirección, en forma regular para asegurar que el alcance siga siendo suficiente y que se identifiquen mejoras al proceso de SGSI. (ICONTEC, 2006,p.15)

Actualizar los planes de seguridad para tener en cuenta las conclusiones de las actividades de seguimiento y revisión. (ICONTEC, 2006,p.15)

Registrar acciones y eventos que podrían tener impacto en la eficacia o el desempeño del SGSI. (ICONTEC, 2006,p.15)

Mantenimiento y mejora del SGSI, de acuerdo con la norma técnica ISO-27001

De acuerdo con la norma técnica ISO-27001 la organización debe, regularmente:

Implementar las mejoras identificadas en el SGSI. (ICONTEC, 2006,p.16)

Emprender las acciones correctivas y preventivas adecuadas de acuerdo con los numerales 8.2 y 8.3.

Aplicar las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y las de la propia organización. (ICONTEC, 2006,p.16)

Comunicar las acciones y mejoras a todas las partes interesadas, con un nivel de detalle apropiado a las circunstancias, y en donde sea pertinente, llegar a acuerdos sobre cómo proceder

Hay que asegurar que las mejoras logran los objetivos previstos. (ICONTEC, 2006,p.16)

Controles

Con la finalidad de hacer seguimiento y monitoreo al sistema de seguridad de la información se crean los siguientes controles:

Diligenciar un documento que indique los días que estará el equipo por fuera de la oficina

Todas las áreas deben tener contraseñas de acceso a la información para los usuarios

Instalar un dispositivo de almacenamiento que permita la disponibilidad, confidencialidad e integridad de la información.

En la matriz de accesos cada usuario debe tener un rol asignado para el ingreso al dispositivo de almacenamiento, lo cual le permitirá Eliminar, crear carpetas, adicionar información, consultar entre otros.

Todos los documentos físicos se automatizarán para establecer archivos por áreas en el dispositivo de almacenamiento y cada usuario tendrá una contraseña para acceder desde cualquier lugar a la información.

Se implementará una red de internet para usuarios internos y una red de internet para visitantes

Los correos electrónicos y equipos deben tener licencia y la política de tratamiento de datos.

Diseñar un cronograma de actualización de software, correo y mantenimiento general de los equipos.

Se deben realizar Backup de información de manera continua

Observaciones de la
administración de
ARFUSOG

Nota. Elaboración propia. Fuente la información fue obtenida de la Norma técnica ISO-27001 (2006).

Requisitos de Documentación

Con respecto al sistema de Seguridad de la Información, la tabla 14 muestra los requisitos de documentales para un SGSI. Tener identificada la documentación requerida para el sistema SGSI, permitirá a la entidad tener claro el paso a seguir para el éxito del sistema y la aprobación por parte de la dirección.

Tabla 11

Requisitos de Documentación para un SGSI

	Requisitos de documentación	Versión 1. 22-10-2022
Objetivo	Articular la dirección de ARFUSOG y las políticas de seguridad de la información con el objeto de que las acciones de la empresa sean articuladas con los objetivos misionales de la organización y que estos queden documentados a través de registros entre otros.	
Alcance	Determinar los documentos necesarios para SGSI en la empresa asociación ARFUSOG	

Requisitos de documentación del SGSI de acuerdo con la Norma Técnica ISO – 27001

La documentación del SGSI debe incluir:

declaraciones documentadas de la política y objetivos del SGSI. (ICONTEC, 2006,p.17)

el alcance del SGSI. (ICONTEC, 2006,p.17)

los procedimientos y controles que apoyan el SGSI. (ICONTEC, 2006,p.17)

una descripción de la metodología de valoración de riesgos. (ICONTEC, 2006,p.17)

Informe de valoración de riesgos. (ICONTEC, 2006,p.17)

Plan de tratamiento de riesgos. (ICONTEC, 2006,p.17)

Los procedimientos documentados que necesita la organización para asegurar la eficacia de la planificación, operación y control de sus procesos de seguridad de la información, y para describir cómo medir la eficacia de los controles. (ICONTEC, 2006,p.17)

Los registros exigidos por esta norma. (ICONTEC, 2006,p.17)

La declaración de aplicabilidad. (ICONTEC, 2006,p.17)

Control de documentación del SGSI de acuerdo con la Norma Técnica ISO – 27001

La documentación que exige la norma ISO-27001, busca proteger y controlar los documentos a través de acciones que lidere la dirección de la empresa que sean necesarias para:

aprobar los documentos en cuanto a su suficiencia antes de su publicación. (ICONTEC, 2006,p.18)

revisar y actualizar los documentos según sea necesario y reprobarlos. (ICONTEC, 2006,p.18)

Hay que asegurar que los cambios y el estado de actualización de los documentos estén identificados.

Hay que asegurar que las versiones más recientes de los documentos pertinentes están disponibles en los puntos de uso. (ICONTEC, 2006,p.18)

Hay que asegurar que los documentos permanezcan legibles y fácilmente identificables. (ICONTEC, 2006,p.18)
Hay que asegurar que los documentos estén disponibles para quienes los necesiten, y que se apliquen los procedimientos pertinentes, de acuerdo con su clasificación, para su transferencia, almacenamiento y disposición final. (ICONTEC, 2006,p.18)
Hay que asegurar que los documentos de origen externo estén identificados. (ICONTEC, 2006,p.18)
Hay que asegurar que la distribución de documentos esté controlada. (ICONTEC, 2006,p.18)
impedir el uso no previsto de los documentos obsoletos. (ICONTEC, 2006,p.18)
aplicar la identificación adecuada a los documentos obsoletos, si se retienen para cualquier propósito. (ICONTEC, 2006,p.18).
Observaciones de la administración de ARFUSOG

Nota. Elaboración propia. Fuente. De la información fue obtenida de la Norma técnica ISO-27001 (2006)

Recursos Necesarios para la Operación, Mantenimiento y Mejora del Sistema SGSI

Con la finalidad de que ARFUSOG, conozca los requisitos necesarios para la operación del Sistema de Seguridad de la Información, se diseña la tabla 15 llamada recursos necesarios para el SGSI, tales como recursos económicos y Administrativos.

Tabla 12

Recursos Necesarios para la Operación del SGSI

Recursos necesarios para la operación del SGSI				
Detalle	**Objetivo**	**Área**		**Costo promedio**
	Crear un comité de seguridad de información, encargado del mantenimiento, mejora y revisión permanente del sistema de seguridad de información.			
Definición de controles por parte de la administración	Identificar los activos de información; definir los controles a establecer para proteger la información y establecer las fechas de auditorías al sistema de información El sistema SGSI debe estar aprobado por la dirección de ARFUSOG	Administrativa	$	0
Capacitación de colaboradores	Capacitar al personal de la empresa asociación ARFUSOG en el diseño, implementación y seguimiento al Sistema de Seguridad de la Información	Administrativo y Operativo	$	3.500.000
Adquisición de un equipo de almacenamiento de la información (Servidor Nas Synology Diskstation Ds720+ Para Empresa)	Mantener la información con Disponibilidad, Confidencialidad e Integridad	Administrativo y Operativo	$	9.500.000
Ingeniero de sistemas	Dicho profesional será el encargado de la instalación del Sistema de	Ingeniería	$	3.000.000

	Seguridad de la Información, asignación de contraseñas de acceso a la información al personal, mantenimiento y actualización de equipos, instalación de software y programas antivirus, diseño de matriz de riesgo de los activos, base de datos, entre otros			
Adecuación de oficinas	Adaptar el lugar donde estarán los equipos que almacenarán la información de la empresa en red, debe estar en un cuarto con aire acondicionado y un sistema de red eléctrica bien estructurado	Ingeniería	$	4.000.000
UPS para servidores	Mantener un sistema de alimentación de energía auxiliar para que en caso de una falla o pérdida de energía se enciende una batería y mantendrá las computadoras y servidores de la empresa en funcionamiento durante las próximas horas, dependiendo de la capacidad del sistema UPS	Ingeniería	$	12.500.000
		Total	**$**	**32.500.000**

Nota. Elaboración propia

Síntesis de las alternativas de solución a nivel técnico y económico

Desde un punto de vista técnico, el SGSI incluye políticas, procedimientos y medidas de seguridad diseñadas para proteger la información contra amenazas internas y externas. Estas medidas pueden incluir el cifrado de datos, la autenticación de usuarios, el control de acceso y la gestión de parches y actualizaciones.

Desde un punto de vista económico, la implementación de un SGSI puede tener costos significativos, como el costo de adquirir y mantener tecnologías de seguridad, el costo de capacitar al personal en el uso de estas tecnologías y asignar un profesional que se encargue del mantenimiento y control permanente de los activos de información. Sin embargo, estos costos pueden ser justificados por beneficios que ofrece el SGSI, como la protección de la información crítica, la reducción del riesgo de pérdida de datos y la mejora de la confianza de los clientes y proveedores.

En última instancia, la implementación de un SGSI es una inversión importante que puede ayudar a proteger activos críticos de una organización, mejorar la eficiencia operativa y garantizar el cumplimiento de las normas y regulaciones aplicables. Aunque puede haber costos asociados con la implementación y el mantenimiento del SGSI, beneficios a largo plazo pueden superar con creces estos costos y garantizar la continuidad del negocio.

A través de las alternativas de solución para del proyecto de investigación se puede decir que la falta de un sistema de gestión de seguridad de la información en la empresa ARFUSOG, Hace propicio que se gestione el diseño de un SGSI que Cubrirá los activos de información identificados para los procesos y áreas de la empresa, tales como bases de datos, archivos de datos, documentación del sistema, manuales de usuario, materiales de capacitación, políticas, procedimientos, formatos, planes de continuidad, datos confidenciales de clientes, papel correspondiente a contratos y calidad de documentos corporativos. Archivos, activos de software correspondientes a aplicaciones de software, herramientas de desarrollo, utilidades, activos físicos correspondientes a equipos de comunicaciones, redes, discos extraíbles y computadoras.

Por otra parte, la alternativa de juicio de expertos permitió la validación de las herramientas de gestión de proyectos que se tuvieron en cuenta dos criterios de calidad “Validez

y Fiabilidad", si bien las herramientas espina de pescado y Diagrama de Pareto, buscan identificar la causa del problema del sistema SGSI, cada una tiene una característica propia que precisa una validación pertinente en cada caso, el experto mide la precisión de la herramienta descartando errores en la investigación, de esta manera da una opinión de acuerdo a con su trayectoria en el tema. los expertos en las herramientas de gestión de proyectos son profesionales en Administración de Empresas que dieron su punto de vista con respecto a las herramientas utilizadas son: Darlin Adelmo Asprilla Murillo, Laurencia Rojas y Ricardo Pineda, docentes Universitarios.

Conclusión

Mediante la propuesta “Diseño de un sistema de Gestión de Seguridad de la Información (SGSI), para la Asociación ARFUSOG, recolectora de residuos sólidos de la ciudad de Sogamoso y teniendo en cuenta la aplicación de herramientas de gestión de proyectos” se concluye que.

Con la aplicación de la encuesta al personal administrativo y operativo en la empresa ARFUSOG, se logró identificar las característica del sistema de Gestión de Seguridad de la información, en la que se hizo énfasis en la herramienta matriz DOFA, donde se halló que el 11,9% conocen la norma ISSO 27001, mientras que el 88,9% de los empleados no tienen conocimiento de la norma, no obstante el 66,7% de los empleados de ARFUSOG, utilizan la memoria USB para el almacenamiento de la información y 22,2% utilizan el drive, mientras que el 11,1% utilizan el disco duro. el 66,7% de los empleados de ARFUSOG, no conocen sobre la ley de protección de datos, con el fin de tener un diagnóstico de la asociación.

Mediante el análisis del sistema de la información y con el fin de determinar posibles alternativas de posibles soluciones del SGSI para ARFUSOG, se aplicaron herramientas de gestión de proyectos como la espina de pescado, los 5 porqués, lluvia de ideas y diagrama de Pareto en el cual se halló que con la aplicación de la matriz de priorización se asignó una valoración a la causa raíz del problema del 12,5% al riesgo que presenta dicha causa para la empresa; en el caso de desafíos de implementación también se asignó la valoración del 12,5%; a las Posibilidades de éxito un 12,5%, a la Conformidad de la administración un 12,5%, Relación con requisitos un 12,5%, a la Urgencia de implementación del SGSI un 12,5% y al acuerdo con las partes interesadas un 12,5% que equivale al 100% de la priorización de la causa que ocasionan el problema en la empresa. Así mismo con la aplicación del diagrama de Pareto se

identificaron y priorizaron las fallas relevantes del sistema de seguridad de la información que tiene la entidad, basado en el principio de que el 80% de los problemas de seguridad de la información se deben a un 20% de las causas subyacentes. Las causas relevantes son las siguientes; desconocimiento de la norma técnica ISO-27001, inexistencia de una matriz de riesgos, conocimiento empírico del manejo de la información.

Estimar las posibles soluciones del sistema de Gestión de seguridad de la información, permitió definir políticas y procedimientos para el acceso a la información de la empresa de manera controlada salvaguardando la confidencialidad, integridad y disponibilidad de los datos y archivos de uso permanente, se hace evidente con las herramientas de gestión de proyectos matriz de priorización de causas y Juicio de expertos como herramienta de evaluación del proceso aplicado. Se logro establecer requisitos y controles de mejora del SGSI para la empresa asociación ARFUSOG, dejando como punto de partida la Norma técnica (ISO-27001), el numeral 02 Enfoque Basado en Procesos, con la cual, se asignó un puntaje a los activos a proteger en el sistema de Información de acuerdo con los niveles de riesgos de la siguiente manera: Muy bajo (0-1); Bajo (2-3); Medio (4-5-6); Alto (7-8); Muy alto (9); Emergencia (10). Además, se establecieron requisitos para la implementación de documentos que cubran todas las actividades relacionadas con la seguridad de la información, incluyendo políticas, procedimientos, instructivos, registros y otros documentos necesarios para la gestión del sistema.

En general, la implementación de un SGSI puede requerir una inversión significativa de tiempo, recursos y dinero. Los costos asociados pueden incluir la contratación de expertos en seguridad de la información, la adquisición de tecnología y herramientas de seguridad, la capacitación del personal y la auditoría y certificación del sistema.

Recomendaciones

Al concluir el trabajo de investigación propuesto para optar al título de Magister en Gerencia de Proyectos resultan recomendaciones y comentarios para futuras prácticas a nivel empresarial y académico:

Que las organizaciones adopten el ciclo (PHVA), "Planificar-Hacer-Verificar-Actuar" como herramienta de mejora continua para establecer políticas de la seguridad de la información de manera que se garantice la eficacia de controles para obtener resultados medibles y comparables.

Asignar un profesional que se encargue de realizar el mantenimiento a los computadores e implementar controles como contraseñas entre otros de tal manera que se preserve la confidencialidad, disponibilidad y la integridad de la información.

Se espera desde la academia, contribuir al campo del conocimiento en cuanto a las herramientas de gestión de proyectos y sistemas de seguridad de la seguridad de la información como medios estratégicos para conversar datos de manera fidedigna.

Referencia Bibliográfica

Aguila, X. (2015). *Análñisis y diseño de un sistema de gestión de la seguridad de la información basado en el criterio de la NTE INEN-ISO/IEC 27001:2011, de un modelo de negocio aplicado en la comercilización y distribución de productos químicos.* Obtenido de Universidad politécnica salesiana sede Guayaquil : https://dspace.ups.edu.ec/bitstream/123456789/10283/1/UPS-GT001168.pdf

Amaya, J. (2004). *El Método Dofa, Un Método Muy Utilizado Para Diagnóstico De Vulnerabilidad*.

Bastar, S. G. (2012). *Metodología de la investigación. 4-92*. Obtenido de obtenido de: file:///D:/U1/Downloads/Metodologia_de_la_investigacion.pdf

Bernal, S. (2018). *Modelo Multicriterio aplicado alña toma de desiciones represenmtables en diagramas Ishikawa.* Obtenido de Universidad distrital francisco José de caldas : https://repository.udistrital.edu.co/bitstream/handle/11349/13894/BernalRomeroSergio2018.pdf?sequence=1&isAllowed=y

Bolaños, E. (Enero- Junio de 2019). *Diagrama de paretto* . Obtenido de Universidad Autónoma del estado de hidalgo: https://repository.uaeh.edu.mx/bitstream/bitstream/handle/123456789/19271/EDT-Diagrama-de-Pareto.pdf?sequence=1&isAllowed=y

Burgasi. (2021). El Diagrama De Ishikawa Como Herramienta De Calidad En La Educación: Una Revisión De Los Últimos 7 Años. *Revista electrónica TAMBARA*, 1212-1230. Obtenido de http://tambara.org/wp-content/uploads/2021/04/DIAGRAMA-ISHIKAWA_FINAL-PDF.pdf

Burgasi. (2021). *El diagrama de Ishikawa como herramienta de calidad en la educación: Una revisión de los últimos. Revista electrónica TAMBARA, ISSN 2588-0977, 1212 - 1230.Editorial Etecé. (5 de Agosto de 2021). Sistema de información.* Obtenido de repository.ucc:https://repository.ucc.edu.co/bitstream/20.500.12494/20367/1/2017_NC_El%20camino%20del%20%C3%A9xito%20de%20las%20encuestas_Caballero.pdf

Caballero, L. (2017). Obtenido de El camino del éxito de las encuentas y entrevistas : https://repository.ucc.edu.co/bitstream/20.500.12494/20367/1/2017_NC_El%20camino%20del%20%C3%A9xito%20de%20las%20encuestas_Caballero.pdf

Cadena, S. &. (2017). *Modelo de un sistema de gestión de la seguridad de la información aplicada a entidades bancarias.* Obtenido de file:///D:/U1/Downloads/CadenaSierraMiguelAngel.2017.pdf

Campos, B. &. (2021). *El uso de diagrama de Ishikawa para identificar las causas de contaminación en la linea de producción de matanza ganalo. La técnica: Revista de las agrociencias(26), 13*. Obtenido de 21. Obtenido de file:///D:/U1/Downloads/DialnetElUsoDelDiagramaDeIshikawaParaIdentificarLasCausas-8232842.pdf

Carrillo, L. (2016). Actualización rétorica de la lengua: el registro. *Revista electrónica de estudios filológicos* , 1-21.

Casa. (2003). *La encuesta como técnica de investigación. Elaboración de cuestionadrios y tratamiento estadíticos de los datos (I). core.ac.uk, 31(8), 527-538*. Obtenido de https://core.ac.uk/download/pdf/82245762.pdf

Colombia, congreso de la república. (Diciembre 31 de 2008). *Ley 1266 de 20086.* Bogotá D. C: Diario Oficial 47.219 de diciembre 31 de 2008. Obtenido de

http://wp.presidencia.gov.co/sitios/normativa/leyes/Documents/Juridica/Ley%201266%20de%2031%20de%20diciembre%202008.pdf

Cordoba, A. (Mayo de 2015). *Diseño y implementación de un SIGSI para el área de informatica de la curaduria urbana segunda de pasto bajo la norma ISO/IEC 27001.* Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/3627/59650050.pdf?sequence=1&isAll

Editorial Etecé. (2023). *Sistema de información*. Obtenido de https://concepto.de/sistema-de-informacion/

El Presidencia de la Republica de Colombia. (1989). *DECRETO 1360 DE 1989.* Bogota D.C: Diario Oficial 38.871 de junio 23 de 1989. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=10575

El presidente de la República de Colombia. ((Noviembre 22 de 2012)). *DECRETO 2364 DE 2012.* Bogota D.C: Publicado en el Diario Oficial 48622 de noviembre 22 de 2012. Obtenido de http://wp.presidencia.gov.co/sitios/normativa/leyes/Documents/Juridica/Ley%201266%20de%2031%20de%20diciembre%202008.pdf

Emprende hoy . (10 de octubre de 2017). *¿ Cómo se desarrolla la empatía en las empresas?* Obtenido de https://rpp.pe/campanas/contenido-patrocinado/como-se-desarrolla-la-empatia-en-las-empresas-noticia-1081654

FIRMA-e.com. (2013). *¿Qué es un SGSI – Sistema de Gestión de Seguridad de la Información?* Obtenido de https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-

informacion/#:~:text=El%20concepto%20clave%20de%20un,riesgos%20de%20seguridad%20de%20la

García. (2003). Mejora continua de la calidad en los procesos. *Redalyc, 6*(1), 89- 94. Obtenido de https://www.redalyc.org/pdf/816/81606112.pdf

García, F. (2019). *Análisis FODA análisis externo y análisis externo* . Obtenido de file:///D:/U1/Downloads/4.%20ANALISIS_DOFA.pdf

García, L. (2019). *Aplicación del mapa de empatía: una herramienta de valor en los modelos de negocio* . Obtenido de https://repository.unimilitar.edu.co/bitstream/handle/10654/35868/Garc%C3%ADaDelgadoLeidyKatherine2019.pdf?sequence=1

Guaman, C. y. (s.f.). Cumplimiento de las políticas de seguridad de información en las cooperativas de ahorro y crédito del cantón Cañar. *Revista de Producción, Ciencias e investigación*. Obtenido de https://www.mendeley.com/search/?page=1&publicationYear=2022&query=SGSI-%2027001%20&sortBy=relevance

Guerra. (2021). Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias. *Información Tecnológíca*, p.1-12. Obtenido de https://www.mendeley.com/search/?page=1&publicationYear=2022|2021&query=SGSI-%2027001%20&sortBy=relevance

Guzman. (2015). . *Diseño de un sistema de seguridad de la información para una entidad financiera de segundo piso.* Obtenido de Obtenido de institución Universitaria Polotécnico: file:///D:/U1/Downloads/Proyecto%20de%20Grado%20SGSI%20-

Hernández. (2016). Juicio de expertos para la validación de un instrument de medición del sindrome de bournout en la docencia. *Revista Ra Ximhai, 12*(6), 327-346. Obtenido de https://www.redalyc.org/pdf/461/46148194023.pdf

ICONTEC. (22 de 03 de 2006). *Norma Técnica Colombiana NTC-ISO-IEC-27001.* Obtenido de Tecnología De La Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad De La Información (SGSI). Requisitos: https://img1.wsimg.com/blobby/go/b653c9ee-535c-4528-a9c5-bb00166ad0dc/downloads/1cd65ml0r_919353.pdf

ICONTEC. (22 de 03 de 2006). *Seguimiento y revisión del SIGSI.* Obtenido de Norma Técnica Colombiana NTC-ISO-IEC-27001: https://img1.wsimg.com/blobby/go/b653c9ee-535c-4528-a9c5-bb00166ad0dc/downloads/1cd65ml0r_919353.pdf

Ishikawa. (1993 citado en Campos, 2021, p.16). Obtenido de http://tambara.org/wp-content/uploads/2021/04/DIAGRAMA-ISHIKAWA_FINAL-PDF.pdf

Martinez, A. (2019). *Importancia de la implementación de un sistema de gestión de seguridad de la información (SGSI) en las empresas bajo la ISO 27001.* Bogotá.

Martinez, L. (10 de Abril de 2012). Marco conceptual en el proceso de investigación. *Scielo*, 146 - 151. Obtenido de Consejo Académico del Área de las Ciencias Sociales. Universidad Nacional Autónoma de México. UNAM. México D.F.,. Scielo, 146-151.: http://www.scielo.org.mx/pdf/iem/v1n3/v1n3a7.pdf

Martínez, R. &. (2012). *Marco conceptual en el proceso de investigación.* Obtenido de Consejo Académico del Área de las Ciencias Sociales. Universidad Nacional Autónoma de México. UNAM. México D.F.,: http://www.scielo.org.mx/pdf/iem/v1n3/v1n3a7.pdf

Martins, J. (4 de 11 de 2022). *¿Qué es el Ciclo Planificar-Hacer-Verificar-Actuar (PHVA)?* Obtenido de https://asana.com/es/resources/pdca-cycle

Mayen, G. C. (octubre de 2018). *Niveles de empatía en los trabajadores de servicio al cliente en una empresa inmobiliaria de guatemala.* Obtenido de http://recursosbiblio.url.edu.gt/tesiseortiz/2018/05/43/Coronado-Gabriela.pdf

Mayen, G. C. (Octubre de 2018). *Niveles de empatía en los trabajadores de servicio al cliente en una empresa inmobiliaria de guatemala* . Obtenido de http://recursosbiblio.url.edu.gt/tesiseortiz/2018/05/43/Coronado-Gabriela.pdf

Mora. (2020). Sistema de gestión de Seguridad de la información bajo la norma NTE ISO- EC 27001 (Instituciones de educación superior). p.1. doi:NISSN 2074-0735

Narvaez, Y. y. (2022). Aplicación de la Norma ISO-27001 para la seguridad de los sitemas de información. p1-17 . Obtenido de https://doi.org/10.23857/dc.v8i3.2854

NQA. (2013). *ISO 27001:2013*. Obtenido de Guía De Implantación Para La Seguridad De La Información: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Presidencia de la Republica de Colombia. (2016). *Decreto 596 de 2016.* Obtenido de squema de la actividad de aprovechamiento del servicio público de aseo y el régimen transitorio para la formalización de los recicladores de oficio: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=69038

Rincón. (2018). *Análisis de la relación- Beneficio en el diseño e implementación del sistema de gestión de calidad Iso 27001 en la empresa GFI Informática colombia S.A.S* . Obtenido de

https://repository.ucatolica.edu.co/bitstream/10983/23172/1/Brayan%20Leonardo%20Guerrero%20Rincon%20Trabajo%20Final%20de%20Grado.pdf

Rojas, R. &. (2015). Válidación por juicio de expertos: dos investigaciones cualitativas en la linguistica aplicada. *Revista nebrija*, 1-16. Obtenido de https://www.nebrija.com/revista-linguistica/files/articulosPDF/articulo_55002aca89c37.pdf

Rosa Martin. (2021). Automatización de un sistema de gestión de Seguridad de la Información basado en la norma ISO-IEC 27001. págs. P. 1- 22.

Russell, J. (2013). *Guia de implementacion para la seguridad de la Información*. Obtenido de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Soewito, R. y. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. *Egyptian informatics Journal*, p 1-22. doi:https://doi.org/10.1016/j.eij.2022.03.001

Técnica NTC-ISO/IE CColombiana 27001, 2006-03-22. (2006-03-22). *Tecnología de la información. técnicas de seguridad. sistemas de gestión de la seguridad de la información (SGSI). requisitos.* Bogota: Editada por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

Yungan. (2022). Aplicación de la Norma ISO 27001 para la seguridad de los Sistemas de Información. *Dominio de las ciencias*. Obtenido de https://www.mendeley.com/search/?page=1&publicationYear=2022&query=SGSI-%2027001%20&sortBy=relevance

Apéndices

Apéndice A

Encuesta

Proyecto	**Diseño de un sistema de Gestión de seguridad de la información (SGSI) para la asociación ARFUSOG**
Objetivo	Obtener información que permita documentar el proyecto
Instrucciones de uso	Lea cuidadosamente la pregunta antes de responder Marque la respuesta con una x Esta encuesta es de carácter confidencial, de la veracidad de su respuesta depende el éxito de la investigación

Sección de preguntas

1**. Conoce usted la norma ISO 27001?**

Si	
No	x

2. Tiene conocimientos sobre el sistema de seguridad de la información?

Si	
No	x

3. Conoce sobre la ley de protección de datos?

Si	x
No	

4. **Cuál es el medio donde almacena los Backup (Copia de seguridad)?**

NAS	
DRIVE	
Disco duro	x
Memoria USB	

5**. Verifica la información una vez realiza el Backup?**

Si	x
No	

6. **La empresa tiene definida políticas de control de la información?**

Si	
No	x

7. Los computadores tienen licencia vigente?

Si	x
No	

8. Cada empleado tiene una contraseña de acceso para su ingreso al sistema de información de la empresa?

Si	
No	x

9. Los equipos de cómputo, donde se almacena la información de la empresa son?

Alquilados	
Propios	x

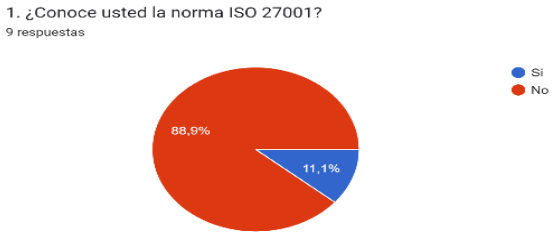
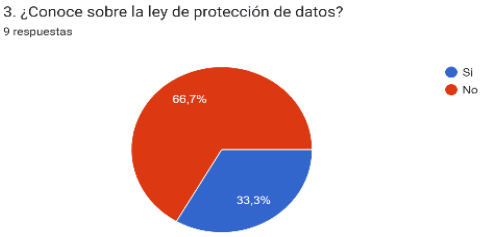
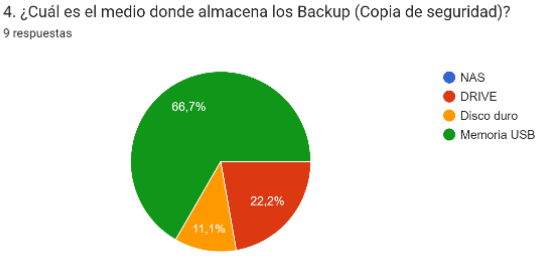
10. Le gustaría que la empresa implementara un sistema de Gestión de Seguridad de la información?

Si	x
No	

Nota. Elaboración propia

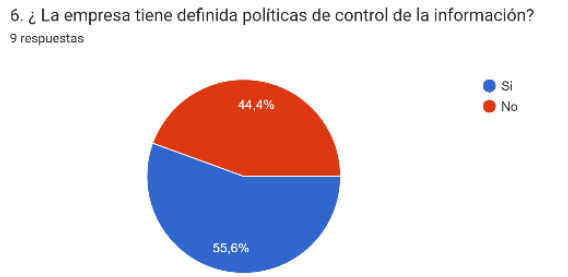
Apéndice B

Análisis de la Aplicación de la Encuesta

Análisis de la aplicación de la encuetas	Grafico de la aplicación de la encuesta
El 88,9% de los empleados de ARFUSOG, no tienen conocimientos de las normas ISO 27001.	
El 88,9 % de los empleados de la empresa ARFUSOG, no tiene conocimiento sobre el sistema de seguridad de la información de la empresa.	
El 66,7% de los empleados de ARFUSOG, no conocen sobre la ley de protección de datos.	
El 66,7% de los empleados de ARFUSOG, utilizan la memoria USB para el almacenamiento de la información y 22,2% utilizan el drive, mientras que el 11,1% utilizan el disco duro.	

El 66,7% de los empleados de ARFUSOG, verifica la información que guardan en el Backup.

El 55,6% de los empleados de ARFUSOG, dice que la empresa tiene definida las políticas de control de la información.

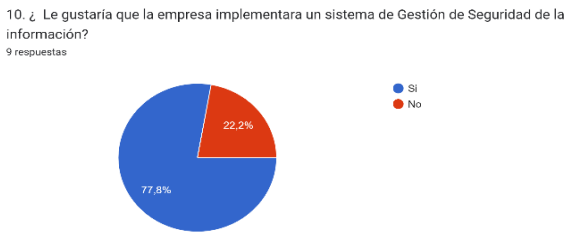


El 100% de los empleados de ARFUSOG, dicen que los computadores de la empresa tienen licencia vigente.

El 88,9% de los empleados de ARFUSOG, no tienen contraseño ni claves de acceso para ingresar al sistema de información de la empresa.

El 100% de los empleados de ARFUSOG, que los equipos computo de la empresa para almacenar la información son propios.

El 77,8% de los empleados de ARFUSOG, les gustaría que se implemente un sistema de gestión de la seguridad de la información de la empresa.



*Nota***.** Elaboración propia