Implementación de un sistema de gestión de seguridad de la información bajo los lineamientos de la norma NTC ISO/IEC 27001:2022 integrada con NTC ISO 9001:2015 y NTC ISO 14001:2015 para el área TI de la empresa Extrucol S.A.

David Fabián Arias Cañas, Henry Alexander Albarracín Montaña

Trabajo para optar el título de Magíster en Calidad y Gestión Integral

Director

Omar Vivas Calderón

Magister en E-learning

Universidad Santo Tomas, Bucaramanga

División de Ingenierías y Arquitectura

Maestría en Calidad y Gestión Integral

2023

Dedicatoria

Dedico la presente tesis principalmente a Dios, por darme el conocimiento y la sabiduría que me guiaron en este proceso.

A mi amor y compañera de vida Malory Pereira, a mi madre Carmen Cañas, a mi tía Isabel Cañas, les dedico este trabajo, por su amor, motivación y apoyo incondicional, que me permitieron seguir adelante en esta constante búsqueda de ser un mejor profesional y ser humano.

Dedico esta tesis de maestría a la memoria de Víctor Julio Cañas Capacho (Q.E.P.D), quien más que un familiar; fue un pilar fundamental en mi vida y mi mayor apoyo. Su legado perdura en cada logro que alcanzo, a pesar de su ausencia física. Su amor, sabiduría, compromiso y dedicación continúan siendo una fuente de inspiración para mí. Siempre lo recordaré con cariño le agradeceré por todo lo que me enseñó.

David Fabián Arias Cañas

Dedicatoria

Quiero comenzar mi dedicatoria primeramente a Dios por permitirme hacer parte de este proceso de aprendizaje y que se dieran las cosas para lograr el desarrollo adecuado del proyecto, también quiero dar agradecimiento muy especial a mis papás (Ana y Henry), a mis hermanos (Andrés y Jessica) y a toda mi familia por apoyarme en cada paso que he dado en mi vida y brindarme ánimos en los momentos más difíciles.

Quiero agradecer también a la familia Gómez Montaña y la familia Amaya López, quienes siempre me brindaron apoyo y ayuda cuando lo necesitaba y finalmente a mis compañeros de clase, a los docentes que hacen parte del programa y al personal de la Universidad Santo Tomás seccional Floridablanca, sin cada una de las personas nombradas anteriormente no sería posible el cumplimiento de este objetivo y el crecimiento mis proyectos de vida.

Henry Alexander Albarracín Montaña

Agradecimientos

Queremos agradecer a nuestro tutor, Omar Vivas Calderón, por su guía y orientación durante el desarrollo de nuestra tesis. Sus comentarios, sugerencias y sobre todo la prontitud con que atendió nuestras solicitudes, fueron de gran ayuda para avanzar y mejorar el proyecto.

Agradecemos a la empresa Extrucol S.A., por permitirnos desarrollar el proyecto de grado y por ende darnos acceso a la información y el tiempo de sus colaboradores para ejecutarlo.

Agradecemos a nuestros compañeros de clase y docentes, por su amistad, las sonrisas causadas y notable apoyo durante estos años de estudio.

Por último, queremos agradecer a la Universidad Santo Tomás seccional Bucaramanga, por brindarnos la oportunidad de realizar nuestros estudios y darnos las herramientas necesarias para crecer profesionalmente y ser mejores seres personas gracias al enfoque humanista que promueve la institución.

Contenido

Lista de tablas

Lista de figuras

Apéndices

Apéndice A. *Organigrama Extrucol S.A. Nota.*

Apéndice B. *Matriz de diagnóstico preliminar.*

Apéndice C. *Informe de auditoría.*

Nota. (Ver archivo en fuente externa).

Resumen

En este estudio, se evidencia el crecimiento que ha tenido la organización Extrucol S.A., quien en sus 35 años de existencia ha tenido un crecimiento exponencial y entendiendo las dinámicas del actual contexto y en busca del cumplimiento de sus objetivos estratégicos decidió hace dieciocho años implementar el sistema de gestión de calidad y posterior el sistema de gestión ambiental, los cuales ha mantenido certificados en el tiempo y actualmente se cuenta con las versiones NTC ISO 9001:2015 y NTC 14001:2015 certificadas.

Actualmente existen diversos sistemas de gestión, cada uno con un propósito de mejora u objetivos diferentes, la gran ventaja es que todos manejan una estructura de alto nivel lo cual facilita una eventual integración de varios sistemas si la organización así lo define.

En la actualidad las organizaciones se encuentran digitalizando su información, no solo por disminuir el impacto ambiental, sino porque posterior a la pandemia ocurrida, es necesario tener la información disponible para no generar ningún traumatismo y operar con normalidad.

Por medio del presente proyecto se planteó el diseño e implementación de un sistema integrado de gestión de seguridad de la información bajo los parámetros de la NTC ISO/IEC 27001:2022 para integrarlos con los sistemas de gestión ya implementados en la organización bajo la metodología de requisitos comunes, para ello se realiza el diagnóstico preliminar mediante el análisis de brechas, el diseño acorde a la metodología del ciclo Deming y la ejecución a través de la documentación e implementación del SIG, y la verificación se validó con un ejercicio de auditoría con un informe como evidencia. El proyectó finalizó articulando los sistemas de gestión mencionados completamente los requisitos de las tres normas, lo cual indiscutiblemente aumenta la confianza y la seguridad de la información de la compañía.

Palabras clave: artículo científico, NTC ISO/IEC 27001:2022, NTC ISO 9001:2015, NTC

ISO 14001:2015, calidad, seguridad de la información, análisis de elementos comunes

Abstract

In this study, we can see the growth that Extrucol S.A. has experienced. In its 35 years of existence, the organization has undergone exponential growth. Understanding the dynamics of the current context and in pursuit of its strategic objectives, it decided to implement the quality management system eighteen years ago, followed by the environmental management system. These systems have been maintained and are currently certified under NTC ISO 9001:2015 and NTC 14001:2015 standards.

Today, there are various management systems, each with different improvement purposes and objectives. The great advantage is that all of them follow a high-level structure, making it easier to potentially integrate multiple systems if the organization chooses to do so.

Currently, organizations are digitizing their information, not only to reduce environmental impact but also to ensure information availability in the post-pandemic era. Having accessible information is essential to operate smoothly and without disruptions.

This project aimed to design and implement an integrated information security management system based on the NTC ISO/IEC 27001:2022 standards. This integration was achieved with the previously implemented management systems within the organization, following the common requirements methodology. The process began with a preliminary diagnosis through gap analysis, designing the system in accordance with the Deming cycle methodology, and implementing it through documentation and the SIG (Security Information Management System). The verification was validated through an audit exercise, with a report as evidence. The project concluded by fully aligning the management systems with the requirements of all three standards, undeniably increasing the company's confidence and information security.

Keywords: scientific article, NTC ISO/IEC 27001:2022, NTC ISO 9001:2015, NTC ISO

14001:2015, quality, information security, analysis of common elements

Glosario

Análisis de riesgos: proceso que implica la identificación, análisis y valoración de amenazas y vulnerabilidades que pueden provocar efectos no deseados. (Safety Culture, 2023)

Auditoría: un proceso de revisión independiente que evalúa la efectividad del SGSI y su cumplimiento con políticas y norma técnica asociada. (UNIVERSITAT RAMÓN LLULL, 2022)

Certificación de seguridad de la información: el proceso de evaluación realizado por un organismo de certificación independiente para validar el cumplimiento del SGSI con estándares y regulaciones aplicables (ICONTEC, 2023)

Controles de seguridad de la información: medidas implementadas para procurar proteger la información, incluyendo controles técnicos, organizativos y físicos. (Regueros, 2023)

Gestión de incidentes de seguridad: proceso para identificar, responder y gestionar incidentes de seguridad, como brechas de datos o ataques cibernéticos. (Sphera's Editorial Team, 2022)

Gestión de proveedores: proceso que implica el seguimiento y supervisión de proveedores de servicios que tienen acceso a la información de la organización. (Certcampus, 2021)

NTC ISO 14001:2015: parte del sistema de gestión usada para gestionar aspectos ambientales, cumplir los requisitos legales y otros requisitos y abordar los riesgos y oportunidades. (ICONTEC, 2015)

NTC ISO 9001:2015: parte del sistema de gestión de la organización enfocada en el logro de los resultados, en relación con los objetivos de la calidad, para satisfacer las necesidades, expectativas y requisitos de las partes interesadas según corresponda. (ICONTEC, 2015)

NTC ISO/IEC 27001:2022: documento que incluye los requisitos para la evaluación y el tratamiento de los riesgos de la seguridad de la información adaptados a las necesidades de la

organización. (ICONTEC, 2022)

Plan de contingencia: planes y procedimientos diseñados para garantizar la continuidad de las operaciones de la organización después de un desastre o evento de ataque cibernético. (Gutierrez y Valencia, 2006).

Política de seguridad de la información: un documento que establece los lineamientos e intenciones de la alta dirección sobre el actuar frente a la seguridad de la información. (IBM, 2021)

Registros de seguridad: documentación detallada de eventos y actividades relacionados con la seguridad de la información, necesarios para el seguimiento y la auditoría. (IBM, 2022)

SGSI (Sistema de Gestión de Seguridad de la Información): conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y proceso para el logro de estos objetivos (ICONTEC, 2015)

Introducción

Los sistemas integrados de gestión son herramientas claves para el óptimo funcionamiento de las organizaciones, que, a través de sus requisitos, guían a las empresas a mejorar en diferentes aspectos, donde cada sistema de gestión tiene un objetivo definido. La estructura de alto nivel que adoptan las normas, hace que la asimilación y la adaptación de las empresas hacia el logro de objetivos y el mejoramiento continuo sea el adecuado.

Extrucol S.A. es una empresa bumanguesa con 35 años de trayectoria dedicada a la fabricación y comercialización de tubería y accesorios de polietileno que se preocupa por blindarse desde diferentes áreas, para evitar que algún evento no deseado se materialice y ponga en riesgo la continuidad del negocio, es por eso que tiene certificado el sistema de gestión en control y seguridad SGCS BASC y se encuentra en proceso de implementación del programa OEA (operador económico autorizado) de la DIAN, los cuales en su estructura, la seguridad en los procesos relacionados con la tecnología y la información tienen una gran importancia, para lo cual implementar un sistema de gestión de seguridad de la información (SGSI) según los lineamientos de la NTC ISO/IEC 27001:2022 le aporta a la compañía a gestionar de una manera más eficiente sus sistemas de gestión ya implementados.

Acorde con el contexto externo de las organizaciones, el cual se ha visto obligado a utilizar cada día más la información de manera digital, donde en Extrucol S.A. a causa de la pandemia SARS-CoV-2 se implementó el 100% de trabajo en casa del área administrativa, el 90% de la información que se tenía en forma física, ahora se maneja de manera digital, lo cual tiene un gran impacto positivo visto desde el punto ambiental, pero aumentan los riesgos de seguridad de la información al encontrarse en la red.

La estructura de alto nivel tiene como objetivo facilitar la comprensión y la aplicación de las normas de sistemas de gestión. También permite a las organizaciones integrar sus sistemas de gestión, lo que puede conllevar beneficios significativos, como una mayor eficiencia y eficacia. (ISO, 2022)

Es por ello que para la practicidad de implementar el sistema de gestión de seguridad de la información bajo el esquema de la norma técnica NTC ISO/IEC 27001:2022, se hará mediante un análisis de requisitos comunes para obtener un sistema que sea viable y fácil de mantener, puesto que transversalmente con los otros sistemas implementados se tiene información homónima para evitar caer en la duplicidad y que en las organizaciones se vuelva tedioso tener implementado más de un sistema de gestión al mismo tiempo.

Inicialmente se realiza un diagnóstico para conocer el grado de implementación del sistema de gestión al inicio del proyecto e identificar que documentación y controles se requieren implementar para cumplir con los requisitos de la norma técnica.

Para implementar satisfactoriamente el sistema de gestión ya mencionado, se cuenta con el apoyo del personal de TI, quienes nos brindan la información para documentar, modificar o actualizar los registros y documentos por parte de los investigadores.

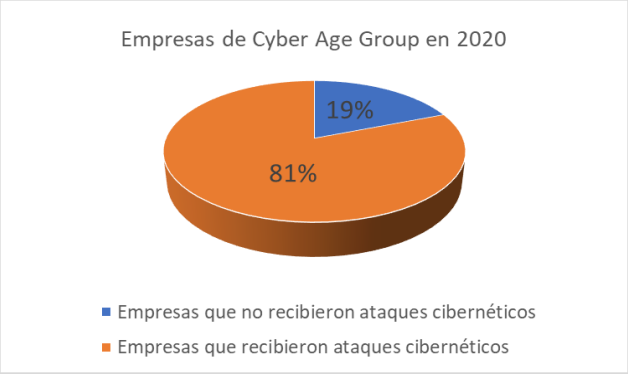
Una vez implementado se somete el proceso de TI a una auditoría realizada por un ingeniero de sistemas con la competencia para realizarla, la cual arroja un resultado positivo.

1. Implementación de un sistema de gestión de seguridad de la información en el área TI de la empresa EXTRUCOL

1.1Planteamiento del problema

Dentro del marco de expansión comercial establecido por los avances estratégicos demandados a nivel global en los últimos años la revolución tecnológica ha tenido un incremento exponencial, generando necesidades importantes en la protección de la información producto de la globalización y a la relevancia que tienen los documentos digitales en las últimas décadas. La información es uno de los tesoros más infravalorados en las empresas, donde se encuentran datos importantes de la compañía, sus procesos, sus partes interesadas y demás elementos que debido a su gran auge en estos últimos años los ciber terroristas intentan atacar, con el fin de exponer públicamente dicha confiabilidad.

Figura 1. *Empresas protegidas por la organización mundial Cyber Age Group*

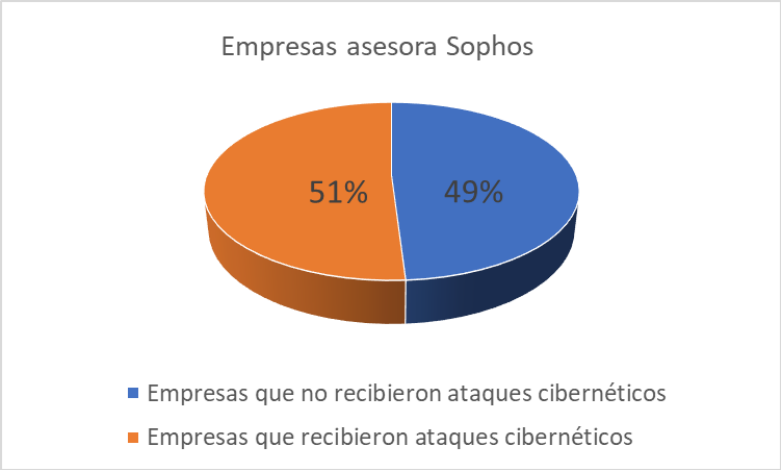


Nota. La figura muestra las cifras de ataques cibernéticos de empresas Cyber age group en el año 2020. Adaptada (La República, 2021).

En el año 2020 según un estudio de Cyber Age Group, el 81% de las grandes organizaciones a nivel mundial fueron víctimas de ataques virtuales, mientras que según la AB Test, hasta noviembre de 2020 se registraron 113 millones de amenazas cibernéticas sin contar

aquellas que accedieron al soborno ya sea pagando o escondiendo su situación debido al gran impacto que puede llegar a tener a nivel mediático, generando inseguridad en sus clientes y dañando la imagen de las empresas, junto con la cantidad de dinero que puede llegar a significar tanto en pago de sobornos como en pago de reconstrucción y mejoras de los sistemas informáticos.

Figura 2. *Empresas protegidas por la organización mundial SOPHOS*



Nota. La figura muestra las cifras de ataques cibernéticos de empresas asesoradas por Sophos en 2020. Adaptada (La República, 2021).

Basados en la encuesta de la reconocida empresa a nivel mundial SOPHOS, quien se dedica a la ciber seguridad, protegiendo a más de 500.000 empresas en todo el mundo, se evidenció que el 51% de ellas sufrieron ataques cibernéticos de diferentes tipos. En Colombia la situación de seguridad informática en las empresas no es ajena a la realidad mundial, a raíz de la pandemia generada se ha evidenciado un gran cambio en la modalidad de trabajo, el cual ha migrado de presencial a teletrabajo o trabajo en casa, razón por la cual las empresas se han adaptado para ofrecer plataformas que permitan acceder a la información desde los hogares de sus colaboradores con equipos adquiridos por la compañía y con softwares específicos para la labor que se debe realizar. A pesar que el trabajo en casa es una herramienta clave para evitar los contagios masivos que la pandemia ha desencadenado, es una gran oportunidad que tienen los delincuentes

informáticos de acechar y conseguir más usuarios para vulnerar su privacidad y atacar su información, razón por la cual en Colombia los ataques aumentaron en un 300% frente a los datos de 2019 según la empresa de ciberseguridad FORTINET, que de la mano de su gerente Juan Carlos Puentes se ha evidenciado el aumento en la asignación de recursos en el tema de seguridad de la información la cual para el año 2020 reportó una pérdida de 3.000 millones de dólares y se prevé que en los próximos dos años, crezca hasta la cifra de 6 billones de dólares, según el FEM. (La República, 2021)

Para efectos de trabajo de este proyecto de investigación se toma como ejemplo la empresa Colombiana Extrusión Extrucol S.A., una organización ubicada en el oriente colombiano que cuenta con 150 trabajadores directos, dedicada a la fabricación, distribución y comercialización de tuberías y accesorios en polietileno con capacidad de respuesta a cualquier municipio del país, a nivel internacional se exporta a Perú, Ecuador, Panamá, Costa Rica, República Dominicana, Honduras, México, Haití, El Salvador, Guatemala e Islas Santa Lucia. Para está empresa objeto de estudio la realidad del panorama nacional frente al aseguramiento de la información es una necesidad inherente que se ha ido incrementando a medida que la empresa ha crecido dentro del mercado global, en la última década está empresa ha incrementado sus procesos fortaleciéndose con políticas de calidad apoyada con la certificación del sistema de gestión de calidad ISO 9001:2015, pero una de las falencias identificadas es que desde el área de TI, no existen controles adecuados y unas buenas prácticas que permitan garantizar la confidencialidad y el aseguramiento de la información para dar cumplimiento a las políticas que la alta dirección de la empresa.

La situación anteriormente nombrada tiene su origen en las siguientes causas:

- No se tiene claridad sobre cómo implementar un sistema de gestión de seguridad de la información. Hace falta identificar e implementar medidas de control que ayuden a

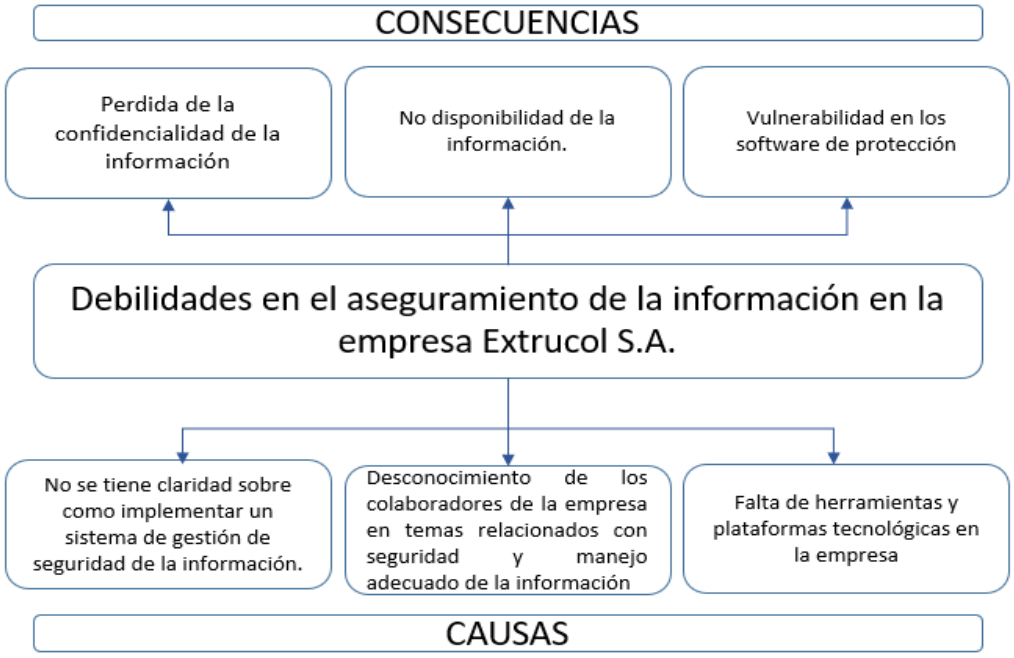
proteger y salvaguardar la información.

- Desconocimiento de los colaboradores de la empresa en temas relacionados con seguridad y manejo adecuado de la información lo cual aumenta la probabilidad que un riesgo o amenaza se materialice.
- Falta de herramientas y plataformas tecnológicas en la empresa, debido a que las amenazas cibernéticas cada vez son más fuertes, los sistemas de información se ven más vulnerables y expuestos, por lo cual se requiere fortalecer los antivirus, servidores, herramientas de control y monitoreo constante que detecten y neutralicen amenazas en tiempo real.

Las causas anteriores han generado el proyecto de investigación que se está abordando, está situación debe mitigarse de alguna manera, de no hacerse, generaría inconvenientes a corto y mediano plazo para la organización, estos efectos son:

- Pérdida de la confidencialidad de la información al no tener controles establecidos que permitan mitigar la fuga o robo de información confidencial o clasificada de la empresa.
- No disponibilidad de la información, puesto que en el momento que exista un robo o secuestro de la información, no se puede tener acceso a ella, generando traumatismo en los procesos de la organización.
- Vulnerabilidad en las aplicaciones software de protección, debido a que cada día los delincuentes cibernéticos se fortalecen para hacer más daño y poder acceder a la información.

Figura 3. *Mapa conceptual de causas y consecuencias sobre las debilidades en el aseguramiento de la información de la empresa Extrucol S.A*



Nota. La figura muestra el análisis de causas y consecuencias de las debilidades del aseguramiento de la información.

1.2 Formulación del problema

¿Cómo implementar un sistema de gestión de seguridad de la información que vincule los requisitos de las normas NTC ISO/IEC 27001:2022 integrada con NTC ISO 9001:2015 y NTC ISO 14001:2015 para el fortalecimiento de los procesos en el área TI de la empresa EXTRUCOL S.A?

1.3 Sistematización del problema

¿Cuál es el estado de cumplimiento actual de los requisitos asociados a las normas NTC ISO/IEC 27001:2022 por parte de la empresa EXTRUCOL?

¿Cómo puede validarse la adecuación, conveniencia y eficacia del sistema de gestión de seguridad de la información diseñado para la empresa EXTRUCOL?

¿Qué aspectos se deben tener presentes para garantizar que el diseño del sistema de gestión integre en forma acertada las normas NTC ISO 9001:2015 y NTC ISO 14001:2015 en pro del beneficio organizacional?

1.4 Justificación

Los sistemas integrados de gestión son herramientas claves para el óptimo funcionamiento de las organizaciones, que, a través de sus requisitos, guían a las empresas a mejorar en diferentes aspectos, donde cada sistema de gestión tiene un objetivo definido. La estructura de alto nivel que adoptan las normas, hace que la asimilación y la adaptación de las empresas hacia el logro de objetivos y el mejoramiento continuo sea el adecuado.

Extrucol S.A. es una empresa que se preocupa por blindarse desde diferentes áreas, para evitar que algún evento no deseado se materialice y ponga en riesgo la continuidad del negocio, es por eso que tiene certificado el sistema de gestión en control y seguridad SGCS BASC y se encuentra en proceso de implementación del programa OEA (operador económico autorizado) de la DIAN, los cuales en su estructura, la seguridad en los procesos relacionados con la tecnología y la información tienen una gran importancia, para lo cual implementar un sistema de gestión de seguridad de la información (SGSI) según los lineamientos de la NTC ISO/IEC 27001:2022 le aporta a la compañía a gestionar de una manera más eficiente sus sistemas de gestión ya implementados.

Acorde con el contexto externo de las organizaciones, el cual se ha visto obligado a utilizar cada día más la información de manera digital, donde en Extrucol S.A. a causa de la pandemia SARS-CoV-2 se implementó el 100% de trabajo en casa del área administrativa, el 90% de la información que se tenía en forma física, ahora se maneja de manera digital, lo cual tiene un gran

impacto positivo visto desde el punto ambiental, pero aumentan los riesgos de seguridad de la información al encontrarse en la red.

El alto índice de ataques a las redes de información al que todo el mundo se encuentra expuesto, donde en Colombia a Julio de 2021 han aumentado un 30% los ataques cibernéticos (Rincón, 2021) se hace necesario e importante diseñar e implementar un sistema de gestión de seguridad de la información (SGSI) que le permita a Extrucol S.A. Gestionar los riesgos a los que se encuentra expuesto mediante la implementación de controles que garanticen la confidencialidad y disponibilidad de la información de la compañía. (Portafolio, 2021).

Contar con un sistema de gestión que controle la seguridad de la información, aporta a elevar la confianza de las partes interesadas de la compañía; las consecuencias de sufrir un robo o secuestro de la información, pueden ser irreversibles, entre las cuales se pueden identificar: pérdida de clientes, daño a la imagen y reputación de la empresa, pérdida irrecuperable de la información, desconfianza de los proveedores, acciones legales de terceros por exposición de información confidencial o sensible.

Según lo anteriormente mencionado, es necesario que en todos los niveles de la empresa se identifiquen los riesgos a los que como organización e individuos se encuentran expuestos, a que se determinen y pongan en marcha controles que aporten a mitigar la probabilidad de materialización de los mismos y que se tenga una ruta definida como plan de acción para detectar oportunamente situaciones que puedan afectar el buen manejo de la información.

En párrafos anteriores se ha detallado posibles causas por secuestro o una intención externa de obtener la información de la empresa desde una óptica delincuencial; sin embargo no se puede pasar por inadvertido la pérdida de información por falta de conocimiento o aquella que se pierde sin ánimos delictivos; es así como toma valor la importancia de implementar la NTC ISO/IEC

27001:2022, la cual a través de sus requisitos ayuda a fortalecer las competencias del personal del área de TI y promueve la adopción de procedimientos, estándares y políticas de todos los integrantes de la empresa, para evitar la pérdida o fuga de información.

1.5 Objetivos

1.5.1 Objetivo general

Implementar un sistema de gestión de seguridad de la información a través de la integración de los requisitos de las normas NTC ISO/IEC 27001:2022 con NTC ISO 9001:2015 y NTC ISO 14001:2015 que permita el fortalecimiento de los procesos en el área TI de la empresa EXTRUCOL.

1.5.2 Objetivos específicos

Identificar el funcionamiento del área TI a través de una caracterización de procesos prioritarios, que establezca el nivel de madurez en la implementación de la norma NTC ISO/IEC 27001:2022.

Definir los elementos para el diseño del Sistema de Gestión de la información a través de la metodología de requisitos comunes de las normas técnicas, de modo que se asegure la integración.

Implementar el sistema de gestión de la información a través del acompañamiento en la ejecución de los lineamientos documentados, de manera que se asegure su asimilación en área TI.

Evaluar el cumplimiento de los requisitos de la norma NTC ISO/IEC 27001:2022 en el área TI de la empresa Extrucol, a través de un proceso de una auditoría interna que determine la

conformidad del sistema de gestión.

2. Marco referencial

2.1 Reseña histórica y caracterización de la empresa

La creación de Extrucol obedeció a la necesidad de desarrollar en Colombia una industria con el propósito de fabricar las tuberías y accesorios para la conducción de gas natural, obedeciendo al interés del gobierno nacional de promover el uso intensivo de este combustible para servicio domiciliario e industrial.

Extrucol fue constituida legalmente en diciembre de 1987 y comenzó su operación en el mes de mayo de 1988, dándose inicio entonces al gran reto que para todos y cada uno de sus funcionarios significaba el ser los pioneros de una empresa con un futuro que debería ser exitoso desde el punto de vista tanto técnico como económico, con la pretensión de Satisfacer las expectativas de sus accionistas, trabajadores y de la Comunidad en general, como cliente potencial de los productos fabricados por la empresa.

Consciente la administración de Extrucol de la responsabilidad que conlleva el suministrar un producto cuyo destino final es la conducción de un combustible con las características del gas natural, desde su inicio orientó sus esfuerzos a incentivar el compromiso de trabajo honesto y de buena calidad, que mereciera la confianza y satisfacción de las empresas distribuidoras de gas como clientes intermedios y del ciudadano colombiano como usuario final.

Con un trabajo de investigación orientado a recopilar en principio las normas y lineamientos existentes a nivel nacional e internacional sobre tubería y accesorios de polietileno para conducción de gas natural, complementado con la participación activa del equipo técnico de

la empresa en los comités del ICONTEC y la participación permanente y objetiva de nuestros clientes, Extrucol comienza a preparar la estructura, los procesos y recursos que conforman el sistema de calidad propio de la organización.

Con un sistema de calidad implementado y con el continuo desarrollo tecnológico de procesos de fabricación, Extrucol estuvo preparado para aceptar los retos de la apertura económica y mereció la confianza del Instituto Colombiano de Normas Técnicas quien otorgó la certificación del sistema de calidad de la empresa, de conformidad con la norma NTC-ISO 9002/94 el 18 de mayo de 1994.

*En el año 2003***:** se diseñan los sistemas de gestión ambiental y de seguridad ocupacional de forma que fueran compatibles con el sistema de gestión existente, y se implementa el SGA buscando su certificación. Por otra parte, el 24 de septiembre de 2003, se actualiza el SGC con la NTC – ISO 9001:2000. Y en Julio 26 de 2006 se renovó el SGA con la NTC-ISO 14001: 2004.

En el año 2007: se logra nuevamente la acreditación del Laboratorio con la norma NTC-ISO-IEC 17025 para 22 ensayos.

En el año 2008: se obtuvo el Sello de Calidad para la Tubería de Polietileno –Aluminio – Polietileno PE-AL-PE con base en la norma australiana AS 4176, así como también el Sello de Calidad con el Reglamento Técnico de la Resolución 1166 del Ministerio de Ambiente, Vivienda y Desarrollo Territorial “MAVDT” para las Tuberías de Agua Potable y Alcantarillado.

En el año 2012: se obtuvo la certificación anual con el ICONTEC para los accesorios importados marca RIFENG y GINDE para PE-AL-PE. Además, se obtuvo el sello de los accesorios de PE socket bajo la norma ISO 8085-1.

En el año 2013: se certificaron con el sello de producto la tubería de PE bajo la NTC 4585 para grandes diámetros (400 mm a 800 mm), en este mismo año se obtuvo la Acreditación del

laboratorio con el nuevo Organismo de Acreditación ONAC bajo la norma NTC – ISO – IEC 17025.

En el año 2014: se obtuvieron los sellos de productos para la tubería multicapa PE-AL-PE y el sistema tubo – accesorio con la norma ISO 17484-1 y la NTC 6015, Al igual que el sello de para la tubería milimétrica bajo los parámetros de la norma UNE-EN 1555-2.

En el año 2015: se certificó la tubería con el sello de redes contra incendios bajo los parámetros internacionales de FM con la norma Class 1613.

En el año 2016: se cambió de ente certificador para los sellos de calidad de producto, de Icontec se pasó a SGS Colombia S.A.S. Además, se obtuvo la declaración de verificación de gases de efecto invernadero (medición huella de carbono) año base 2014.

En el año 2017: se amplió el alcance del sello de redes contra incendios.

En el año 2019: se obtuvo el Sello de Calidad con el Reglamento Técnico de la Resolución 0501 del Ministerio de Ambiente, Vivienda y Desarrollo Territorial “MAVDT” para las Tuberías de Agua Potable y Alcantarillado.

En el año 2020: se realiza una ampliación a las instalaciones permanentes de la empresa, con el fin de tener espacios de trabajo adecuados y acordes a las necesidades actuales de la compañía.

En el año 2021: la empresa cuenta actualmente con 150 empleados, tiene sus instalaciones permanentes en el kilómetro 3 vía palenque - Café Madrid Parque Industrial I de Bucaramanga - Santander - Colombia.

Extrucol S.A. cuenta los siguientes objetivos documentados en su planeación estratégica existente:

- Crear y mantener relaciones de impacto que garanticen negociaciones de largo plazo

- Alinear la organización con la tecnología necesaria que apoye los procesos críticos.
- Mejoramiento y optimización de áreas
- Mejoramiento de procesos internos
- Mantenimiento y fortalecimiento del sistema integral de gestión
- Formación continua y capacitación del personal
- Focalizar la empresa a la nueva estrategia
- Aumentar la rentabilidad operativa.

Figura 4. *Reseña histórica de la empresa Extrucol S.A.*

Nota. La figura muestra la reseña historia de Extrucol S.A. 2020 Adaptado: (Extrucol S.A., 2023).

Organigrama Extrucol

(Ver apéndice A).

2.2 Antecedentes

2.2.1 Antecedentes en el ámbito internacional

En el año 2020 la Universidad Latina de Costa Rica publicó el proyecto de Maestría titulado Propuesta mediante la normativa ISO 27001 para la gestión de la seguridad de la información en la empresa Udersol en Costa Rica y cuyo autor es Gilberto Esteban Solano Méndez. La empresa Udersol brinda servicios tercerizados a una empresa matriz ubicada en San José, Costa Rica que no cuenta con ningún tipo de lineamiento y normatividad y tiene un gran potencial de expansión, por esta razón se quiere aportar al crecimiento de la empresa, generando una propuesta que permita vincular normativa en seguridad de la información en la empresa y de esta manera mejorar la seguridad de la empresa a nivel informático. Para la realización de dicha propuesta, se utilizan herramientas de observación directa en la empresa pero la empresa cuenta con muy poca capacitación y conocimiento de las normativas tanto por parte del CEO como de los colaboradores, factor que dificulta muchos aspectos de la investigación, pero permite explicar de forma clara el proceso que se va a realizar, empezando por una serie de preguntas en formato de cuestionario para el CEO donde se busca conocer el estado de la compañía y los detalles necesarios para proseguir con la propuesta. Posteriormente se busca un ciclo de mejora continua basado en la normativa de la NTC ISO/IEC 27001:2013, donde se quiere implementar y de esta manera Udersol pueda mantener como guía planear, implementar, monitorear e incluso realizar los cambios respectivos a la alineación de la empresa. Adicionalmente se utilizan políticas y controles de corto plazo que tengan un costo bajo buscando una mayor rentabilidad y obtener el mayor beneficio de esta propuesta sin hipotecar la empresa.

La empresa Udersol busca mantener la operatividad de la empresa pero contando con

sistemas que permitan proteger la información de la empresa, pero como primera fase se realiza el diagnóstico de la empresa donde se evidencia una carencia de conocimientos significativa, posteriormente a realizado una introducción al tema por parte del CEO, se procede a realizar una planificación, basados en la misma se busca tener una serie de controles tanto físicos como lógicos que permiten gestionar el riesgo de una manera más segura. La herramienta que se utiliza es el ciclo PHVA (Planear, Hacer, Verificar y Actuar), donde se busca explicar cómo funciona y de esta manera el personal pueda implementar mejoras por su cuenta utilizando esta herramienta de manera óptima. (Méndez, 2020)

En el año 2015 la universidad de Valladolid publicó el proyecto para optar al grado de Ingeniería en organización industrial titulado Cómo gestionar la seguridad de la información (según ISO 27001:2013) en una PYME del sector de las tecnologías de información y comunicación a cargo de los estudiantes de pregrado Abad Peña y María Belén, donde se muestra una guía que permite a las pequeñas y medianas empresas (PYMES) adquirir más conocimientos sobre la norma, su aplicación y la posibilidad de certificarse. Inicialmente desarrollando los conceptos de la norma detallando sus ventajas y el por qué se debe hacer, adicionalmente, se utiliza la metodología PHVA para el mejoramiento de los procesos que se puedan llegar a implementar con la guía que se proporciona. La planeación del proyecto es clave, ya que al detallar el riesgo que pueden tener las empresas, se concientiza a las PYMES la importancia de la información que manejan las empresas y la relevancia que toma al momento de detectar una oportunidad de crecimiento donde la documentación de la misma nos ayuda a planificar los pasos que puede dar la compañía en el futuro y a su vez protegiendo los datos indispensables de la empresa. El proyecto enfatiza en los riesgos se puede presentar la implementación del sistema de gestión de la información ISO 27001:2013, analizando no sólo los posibles riesgos, sino las causas de las cuales

estos se desprenden y cómo podemos atacarlos con el fin de mitigarlos y en mejor de los casos reducir la probabilidad de materializarse al mínimo. Posteriormente se definen los respectivos controles que permitan mantener controlados los riesgos de las empresas proporcionando un ambiente tranquilo y con riesgos, pero siempre manteniendo cada proceso documentado y socializado tanto por la alta dirección como por los colaboradores que se vean implicados en los cambios y controles que previamente se han establecido. Se realiza un control documental y se relaciona con las condiciones actuales de las empresas con el fin de organizar la información de la compañía, buscar los puntos débiles que presentan y fortalecer desde las competencias de los colaboradores con capacitaciones como las de la alta dirección enseñándoles la importancia de los sistemas de gestión y particularmente la norma relacionada con los sistemas de información y finalmente se verifica el desempeño del proyecto con una evaluación por parte de la alta dirección y el personal encargado de supervisar el desarrollo del proyecto. Como se puede observar, el proyecto que se desarrolló, aplicó el ciclo PHVA y realizó la metodología adecuada para implementar un sistema de gestión, sin embargo, al momento de realizar una implementación más rigurosa, se deben tener en cuenta cambios y aspectos que afectan de sobremanera a las empresas, pero a su vez permite una mayor efectividad en el desarrollo de la implementación. (Peña y Belén , 2015)

En 2020 en la universidad César Vallejo de Lima Perú, publicó el proyecto de maestría titulado Implementación de la norma ISO 27001 en el departamento de tecnología de la información de la empresa Esvicsac, Callao a cargo del estudiante Edwin Samuel Arias que implementó la norma ISO 27001:2013 en la empresa Esvicsac debido a que los activos de información en la empresa no se custodian de la mejor manera, siendo un apartado clave en el desarrollo de la actividad, para ello se busca emplear como guía la norma ISO 27001:2013 como

una solución que dificulte la pérdida de información ya sea por ataques cibernéticos o por el mismo descuido de los miembros de las compañías que manejan información valiosa y no tienen estipulados controles para el manejo seguro de información. La investigación utilizó herramientas como entrevistas directas, observación y análisis documental para la primera fase de recolección de datos, permitiendo conocer de primera mano las condiciones de la empresa y las capacidades del personal que en ella laboran, partiendo del jefe de TI, especialista de desarrollo y especialista en infraestructura donde en general la respuesta a la implementación de la norma NTC ISO 27001:2013 fue excelente, ya que son conscientes de la importancia de la información y están prestos a colaborar con todo lo que sea necesario para aportar a la implementación de la norma en su empresa. Posteriormente se empieza la implementación de la norma, desarrollando lo planeado añadiendo los documentos que hacían falta en la papelería correspondiente al sistema utilizando los recursos planeados y se socializa con las áreas involucradas en cada procedimiento que permita dar a conocer todos los cambios que se van a realizar y finalmente se procede a verificar el impacto de la implementación previamente realizada, para finalmente dar un informe a la alta dirección, comunicando directamente los cambios realizados y las condiciones actuales de la empresa. (Quispe, 2020)

2.2.2 Antecedentes en el ámbito nacional

En el año 2016, el estudiante Ronald González publicó en su proyecto de especialización titulado Diseño del sistema de gestión de seguridad de la información (SGSI) para el área de tecnología de la empresa Bakertilly Colombia Ltda. de la ciudad de Bogotá, bajo la norma ISO 27001:2013, propone el diseño de un sistema de gestión de seguridad de la información (SGSI) para el área de tecnología de la empresa Baker Tilly Colombia Ltda. de la ciudad de Bogotá, bajo

la norma ISO 27001:2013, donde se provee prácticas apropiadas para el desarrollo e implementación de cada uno de sus componentes, estableciendo las fases, documentación y procedimientos requeridos y exigidos en el estándar para continuar con el diseño del SGSI de una manera adecuada, en su trabajo, aborda la implementación del sistema de gestión desde la identificación y análisis de los riesgos a los que la empresa se encuentra expuestos y sobre la necesidad de implementar controles que ayuden a mitigarlos. Para el desarrollo de la implementación del sistema de información se procede a realizar el manual para implementar la norma ISO 27001:2013 para el área de sistemas en la empresa donde se revisan las políticas actuales de seguridad de la información con el fin de verificar la funcionalidad de las mismas ya que es una de las claves para mantener controles efectivos y así proteger la información de la compañía. El alcance cubre todos los procesos tanto internos como externos que se encuentren vinculados a la entidad, divulgando las políticas antiguas como las nuevas que cumplan con la efectividad necesaria para garantizar la seguridad de la información en las diversas áreas y procesos. Posteriormente se analizan los aspectos organizativos como son los aspectos documentales, para ello, se basan en las diferentes tareas como la asignación de funciones y responsabilidades; esto permite tener una mayor eficiencia en la administración. Como conclusión, plantea que la implementación de un Sistema de Gestión de Seguridad de la Información - SGSI en la empresa Baker Tilly Colombia Ltda., brindará seguridad en los sistemas de información e incrementará la confianza tanto de sus funcionarios como de sus clientes mejorando su imagen ante ellos generando solidez de la misma. (Garía, 2016)

En el año 2014 la universidad Pedagógica y Tecnológica de Colombia seccional Tunja publicó el proyecto de grado titulado Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia) a cargo de los estudiante Julián

Monsalve, Fredy Aponte y David Chaves que busca estudiar las vulnerabilidades informáticas en una empresa privada, información que nos permite descubrir diversos factores que pueden afectar la seguridad de la compañía y posiblemente nos permitan conocer amenazas de las cuales no nos percatamos. Partiendo por el respectivo diagnóstico donde se encuentran controles relacionados al manejo de contraseñas y seguridad de acceso a la información como base del sistema de gestión de vulnerabilidades con el fin de detallar los controles desde la minucia para reducir los riesgos en cuanto a la vulneración del sistema de información. Los sistemas de operación son claves ya que se analizan las áreas más recurrentes y con mayor relevancia en cuanto al uso de la información y la discreción con la que se maneja la información como es la alta dirección, el departamento de ventas y de proveedores, quienes manejan datos claves de las personas que le compran a la empresa, sus datos financieros y demás; para buscar su protección se realizan cambios en cuanto al uso de papel físico y el uso de softwares de protección que cuiden la información importante en las áreas más discretas de la compañía. Para culminar la investigación, se automatizan ciertos controles al momento de acceder a los dispositivos que cuentan con los datos importante de la compañía como son las claves únicas para el personal específico del área de trabajo, también la restricción a los archivos que no correspondan a su área o responsabilidades, permitiendo así restringir el acceso a la información a personas que no cuentan con la autorización y de esta manera se aplica un control adicional a las cifras de la compañía. (Monsalve, et ál., 2014).

En el año 2016 la universidad abierta y a distancia presentó el proyecto de especialización titulado Diseño de un sistema de gestión de seguridad de la información SGSI- bajo la norma ISO/IEC 27001:2013 para la empresa “En línea financiera” de la ciudad de Cali-Colombia Diseño de un sistema de gestión de seguridad de la información SGSI- bajo la norma ISO/IEC 27001:2013 para la empresa “En línea financiera” de la ciudad de Cali-Colombia a cargo del estudiante Juan

Carlos Oidor donde se diseña un sistema de gestión de seguridad de la información bajo los lineamientos de la norma ISO/IEC 27001:2013 en la empresa “En línea financiera” para optar al título de especialista en seguridad informática, donde se busca cumplir los requisitos legales y documentales para gestionar los activos físicos y tecnológicos que permitan asegurar el uso de la información de manera segura. Se dio inicio al proyecto realizando la gestión del riesgo de la empresa en cuanto al manejo de los datos empresariales, así como la importancia de los documentos manejados según las áreas, donde los documentos de la dirección son claves para la empresa, así mismo la información del área de compras y ventas ya que se manejan datos de clientes y proveedores. Se realizan campañas de concientización para el personal de la empresa, donde se busca que aprendan la importancia de cada documento que manejan y el respectivo uso que debe tener, también la importancia de los controles que se implementan desde la alta dirección para proteger la información. Se encontró que la empresa no cumple con ciertos requisitos legales, siendo un tema clave para la empresa porque el control documental no realizó la respectiva revisión que garantiza a la compañía el cumplimiento total de los documentos obligatorios. Este proyecto nos brinda una guía para revisar no sólo el cumplimiento de los controles de la información, sino también el cumplimiento de los requisitos a nivel legal y organizacional. (González, 2016).

2.2.3 Antecedentes en el ámbito local

El proyecto de especialización titulado Diseñar un Sistema de Gestión de la seguridad de la información (SGSI) a la empresa UNITRANSA S.A. ubicada en la ciudad de Bucaramanga, para el cual realizaron un diagnóstico donde a través de encuestas aplicadas a los trabajadores de la compañía se les preguntaba sobre conceptos específicos de seguridad de la información la cual cerca del 50% de los trabajadores no conocían claramente el significado de estos conceptos. Se

realizó un estudio de la infraestructura y la seguridad física de la empresa, lo cual se encuentra ubicada en el parque romero de Bucaramanga, el cual es asociado a una zona de alta peligrosidad o robos constantes, sumado a la vulnerabilidad que presentan las instalaciones al tener equipos de cómputo, inclusive el servidor al alcance de cualquier tercero y directamente en el piso lo cual puede ser muy riesgoso si llegase a existir alguna inundación por rotura de alguna tubería. En el trabajo se realiza una identificación y valoración de activos informáticos importantes para la empresa en busca de establecer controles que ayuden a mitigar la probabilidad de materialización de los nuevos riesgos detectados. En las conclusiones del proyecto se establece que la información de la empresa Unitransa S.A. se encontraba expuesta en alto grado, por el manejo que se le estaba dando, el tipo de tecnología utilizada, el desconocimiento del personal, la infraestructura, la ubicación geográfica y la falta de políticas. Sin duda el diseño de ISO 27001 aparece como una herramienta que le puede brindar a la empresa a salvaguardar su información. (García y Castro, 2017)

La universidad Santo Tomás seccional Bucaramanga en el año 2016 publicó el proyecto de grado titulado Implementación de un estándar de calidad para la seguridad de la información en la empresa INSURCOL Ltda bajo la norma ISO 27001:2013 a cargo de los estudiantes Patricia Camacho. La empresa se dedica a realizar proyectos de origen civil, mecánico, instrumentación y sector del petróleo a nivel nacional; para este proyecto se empieza contextualizando la importancia de los sistemas de gestión a los colaboradores involucrados en la implementación del sistema, posteriormente se identificaron los activos de la información de la empresa y los posibles riesgos que tienen no sólo en cuanto a la pérdida de la información sino en la organización de la misma con el fin de tener un fácil acceso. Basados en los análisis previos que determinan las condiciones de la compañía, se proponen mejoras en la infraestructura, los equipos y los procedimientos de

seguridad, ya que se presentan problemas de búsqueda de la información al guardarla en desorden y sin llevar controles de guardado para los documentos virtuales. Finalmente se plasman las mejoras propuestas en un plan que permita asegurar el manejo de la información en la empresa, se plasman políticas de seguridad informática que se socializan con el personal para reducir al máximo el riesgo de pérdida y la facilidad de acceso a dichos archivos. (Rojas, 2016)

2.3 Marco teórico

2.3.1 Ciclo de Deming

William Edwards Deming, introduce e implementa su teoría de calidad la cual se basa en un mejoramiento constante, el cual busca mediante su metodología un análisis constante de todas las actividades que impactan a las organizaciones para controlarlas y mejorarlas continuamente.

La metodología de mejoramiento continuo o el llamado ciclo de Deming (P-H-V-A), toma credibilidad a partir del crecimiento exponencial que tiene Japón gracias a la implementación de los modelos de calidad impartidos por el estadista estadounidense posterior a ser devastada en los ataques de Hiroshima y Nagasaki durante la II guerra mundial.

ISO (International Organization for Standardization) reconoce lo valioso de la teoría y la adopta en la estructura de los diversos sistemas de gestión, la cual distribuye en medio de sus requisitos. La norma NTC ISO 9001:2015 tiene como modelo ya mencionado el ciclo de mejoramiento continuo a través de sus 10 capítulos y dentro del capítulo 8 de operación maneja su propio ciclo de PHVA.

2.3.2 Sistema de gestión

Un sistema de gestión se define básicamente por ser un modelo general de procesos y procedimientos que adoptan las organizaciones de tal forma que se asegure realizar todas las actividades necesarias de la mejor manera, pues su estandarización conlleva a cumplir con sus objetivos.

Es una herramienta que permite convertir en hechos las ideas o intenciones de la alta dirección, el cual guía a las empresas a través de sus requisitos a identificar claramente su alcance, sus objetivos, realizar todas las actividades gestionando los riesgos que se puedan presentar y de esta manera mitigar la probabilidad de materialización de eventos no esperados; incentiva la innovación y la mejora continua con el fin de buscar la optimización y efectividad de los procesos.

2.3.2.1 Integración de sistemas de gestión. La integración de sistemas de gestión es un método que permite unificar la información presente en diferentes sistemas de gestión ya existentes en una empresa, garantizando la fiabilidad de los datos sin generar traumatismos ni duplicidad de información en las organizaciones, es por eso que desde la actualización de la NTC ISO 9001:2015, se empezó a adoptar una estructura de alto nivel en los sistemas de gestión, lo cual busca una sincronización o coherencia entre los diferentes sistemas, manteniendo la independencia que se requiere.

2.3.3 ISO 27001:2022

Es una norma internacional que permite la confidencialidad e integridad de la información en las empresas y en los procedimientos que la componen permitiendo a la compañía la evaluación del riesgo y la aplicación de controles necesarios para cumplir el objetivo de dicha norma,

complementándose con buenas prácticas por parte de la organización en materia de capacitación y de los colaboradores como prácticas preventivas que eviten poner en riesgo la información de la empresa.

2.3.4 Seguridad de la información

La seguridad de la información tiene como objetivo mantener la integridad, confidencialidad y disponibilidad de la información mediante diversas herramientas como las políticas de seguridad de la información, softwares especializados para proteger los documentos de ciertos archivos maliciosos y concientización por parte de las empresas que permitan a los colaboradores ser cada vez más conscientes de los documentos que ingresan a sus dispositivos. La seguridad de la información mantiene controles correctivos, pero también preventivos, que en este caso tienen mayor importancia que los controles correctivos, ya que al momento de una filtración por más pequeña que sea, puede generar daños irreparables a la compañía incluyendo documentos físicos.

2.3.5 Políticas de seguridad de la información

Es la declaración ejecutiva de la dirección con respecto a un tema específico que muestra la posición de la compañía, donde varía el alcance según el área, los funcionarios que tenga, el riesgo que presente, la exposición al público, etc, y cuyo objetivo es minimizar los riesgos en las funciones claves de la entidad, acatar los principios de la seguridad de la información, mantener la confidencialidad de la información tanto dentro de la empresa como afuera, proteger los activos tecnológicos de la compañía y establecer guías para los procedimientos delicados en la empresa.

3. Diseño metodológico

3.1 Metodología

Para la ejecución del presente estudio se ha definido seguir la metodología de Análisis de Elementos Comunes con la articulación de las actividades propuestas basadas en el ciclo Deming o ciclo PHVA propuesta por (Palacios Guillem, et ál, 2019). Siendo dos perspectivas muy paralelas, es un método muy adecuado, pues es parte del pensamiento de la estructura de alto nivel que manejan los actuales sistemas de gestión, el cual denota elementos homólogos en las diferentes normas que le permite a las organizaciones contar con una articulación más práctica, evitando duplicidad de documentos y reprocesos. Pese a que, en el estudio realizado de la metodología anteriormente descrita, ésta no fue aplicada directamente en la integración de un sistema de gestión basado en las normas NTC-ISO 9001:2015 y NTC-ISO/IEC 27001:2022.

De esta forma el planteamiento metodológico propone cuatro (4) fases, que a su vez están constituidas por las siguientes actividades específicas:

3.1.1 Fase de planificación

Relacionado al ciclo de mejora continua PHVA la primera fase corresponde a la planeación del diseño del Sistema Integrado de Gestión. Esta fase está integrada por las siguientes actividades principales:

3.1.1.1 Compromiso de la alta dirección. La alta dirección de EXTRUCOL S.A. decide comprometer los recursos y tiempos asociados al logro del objetivo de diseñar e implementar un Sistema Integrado de Gestión que asegure el cumplimiento de los requisitos legales y normativos de calidad y seguridad de la información. Los directivos de la compañía reconocen las ventajas de implementar un sistema de gestión y como este aporta al crecimiento de la misma. Adicionalmente el área de TI reconoce la necesidad de implementar la norma NTC ISO 27001:2022 y se demuestra su interés y disponibilidad lo cual impactará de manera significativa el normal desarrollo del presente proyecto.

3.1.1.2 Diagnóstico preliminar. Se plantea la ejecución de un diagnóstico del estado actual de cumplimiento de los requisitos de las normas NTC-ISO 9001:2015, NTC ISO 14001:2015 y NTC-ISO/IEC 27001:2022 (contemplando los requisitos de los 10 capítulos), así como, el estado y aplicabilidad de los controles de seguridad de la información sugeridos en el Anexo A de la norma NTC-ISO/IEC 27001:2022. Para ello, se propone la realización de un análisis de brecha que permita identificar el nivel de cumplimiento de cada requisito posterior a la verificación de las evidencias objetivas disponibles, culminando con un registro que indique la valoración porcentual del nivel de cumplimiento, tomando como guía la valoración porcentual de la descripción de los niveles de madurez sugeridos en (ICONTEC, 2021). Para cada norma se generará una hoja de cálculo y un análisis de brecha a través de la identificación gráfica de los resultados en un esquema tipo radar. En las siguientes tablas se muestran la estructura de la hoja de cálculo a aplicar, así como, los criterios de categorización y un ejemplo de la esquematización gráfica de los resultados.

Tabla 1. *Estructura general hoja de cálculo análisis de brecha de las normas NTC-ISO 9001:2015, NTC ISO 14001:2015 y NTC-ISO/IEC 27001:2022*

Requisitos de las normas técnicas	Descripción de aplicación de requisitos	Estado*	Responsable de cumplir con el requisito
Requisito evaluado	Descripción de cumplimiento de requisitos	Valoración del estado de implementación.	cargo asociado

Nota. El estado se determina a partir de la verificación de la evidencia o soporte de implementación y su valoración respecto a los criterios de calificación.

Ejecutado el diagnóstico del estado de cumplimiento de cada ítem para ambas normas y del Anexo A, se revisará y analizará el porcentaje de cumplimiento bajo los siguientes criterios.

Figura 5. *Valoración*

Calificación	Criterio	Color
Sin implementación	No es cierto, ocurre en un 0%, la práctica no se encuentra o no ha comenzado todavía, no ocurre nada.	
Poca implementación	Relativamente cierto, ocurre en un 25% aproximadamente, la práctica sólo se ve en algunas áreas.	
Implementación parcial	Parcialmente cierto, ocurre en un 50% aproximadamente, es una práctica común, pero no la mayoría de áreas.	
Prácticamente adoptado como rutina	Cierto en la mayor parte, ocurre en un 75% aproximadamente, la práctica es muy típica, con algunas excepciones.	
Implementado totalmente como rutina y efectivo	Sí, cierto en todas las partes, ocurre en un 100% o casi. La práctica se despliega en toda la organización.	
No Aplicable	Requisito no aplicable de acuerdo al alcance del SIG	

Nota. Criterios de valoración de las evidencias o soportes de implementación. Adaptado (ICONTEC, 2021).

Como complemento para el análisis, los resultados de cada capítulo se esquematizarán en

un gráfico tipo radar.

3.1.1.3 Diseño del sistema integrado de gestión. Anexo al resultado derivado del ejercicio diagnóstico, se procederá a realizar el análisis de relación uno a uno, entre los requisitos de las tres normas, siguiendo para ello la siguiente categorización de los niveles de correspondencia o relación:

Relación total (T): para este caso el requisito de la norma NTC-ISO/IEC 27001:2022, ya está contemplado por algún requisito de las normas NTC-ISO 9001:2015 Y NTC 14001:2015. Para este escenario, no se necesitará la implementación de ningún elemento específico para una u otra norma.

Relación parcial (P): para este caso, el requisito de la norma NTC-ISO/IEC 27001:2022, detalla o especifica alguna medida particular respecto a lo que establece el requisito para las normas NTC-ISO 9001:2015 y NTC 14001:2015.

Inexistencia de relación (X): para este particular los requisitos corresponden a aquellos específicos al objeto y campo de aplicación de las normas respectivas.

El análisis de relación, se complementará con el plan de trabajo que deberá diseñarse con el fin de lograr el cumplimiento total de los requisitos. Estos planes de acción no solo aportarán al cierre de necesidades particulares de cara al cumplimiento de un requisito de una norma, si no, en los casos que así corresponda, darle el alcance correspondiente para el aseguramiento de la integración. De esta forma, los planes serán determinantes en la fase de ejecución.

A continuación, se describe la estructura del anexo de análisis de relación y planes de acción.

Tabla 2. *Estructura general del anexo de análisis de relación de requisitos y plan de acción*
Estructura general del anexo de análisis de relación de requisitos y plan de acción

Capítulo	Requisito	Estado*	Tipo de relación	Plan de acción	Responsable de cumplir con el requisito
Sección de la norma evaluada	Requisito evaluado	Valoración del estado de implementación	Relación total (T) Relación parcial (P) Relación inexistente (X)	Descripción del plan de acción para asegurar cumplimiento o integración	cargo asociado

La primera fase incluye también la generación del plan detallado de integración, que incorporará un cronograma detallado de los elementos de requisitos de norma y las actividades puntuales de integración a realizar, siguiendo las etapas del ciclo PHVA. Se identifican en el plan de trabajo, los recursos asociados (personal, tiempo). Finalmente, la fase cierra con la revisión, ajuste y documentación de los lineamientos del nuevo Sistema Integrado de Gestión (Manuales, políticas, programas, planes, procedimientos, instructivos, anexos, documentos externos, formatos, etc.), surtiendo las respectivas etapas de revisión, aprobación y publicación.

3.2.1 Fase de ejecución

Esta fase incluirá todas las actividades asociadas a la implementación del Sistema Integrado de Gestión diseñado en la fase anterior. Constituye una fase importante que comprenderá la aplicación de modificaciones resultado de las necesidades previamente identificadas. Dentro de esta fase se incluyen las siguientes actividades:

3.2.1.1 Implementación del sistema integrado de gestión. La fase de ejecución reúne varias actividades que resultan determinantes para el impacto esperado por la organización. De allí que, durante la ejecución de implementación se sugiere disponibilidad y trabajo en equipo con el personal de EXTRUCOL S.A. Siendo que uno de los elementos cruciales en el éxito de la implementación del SIG, surge de la promover una cultura de seguridad por parte de todos los colaboradores, por tanto es indispensable fortalecer en el recurso humano los controles que se aplicaran en busca de lograr una articulación práctica y funcional de los sistemas de gestión donde se logre blindar la información teniendo en cuenta que dicho proceso trae consigo la gestión del cambio organizacional y ante todo la sensibilización de la importancia de un compromiso con la implementación de forma permanente y sostenida en el tiempo.

Adicionalmente, a lo largo del proceso de implementación se sugiere mantener un acompañamiento permanente que permite realizar el aseguramiento de la implementación, a través de la verificación periódica de las evidencias del control operacional, el control de riesgos y el cumplimiento de requisitos normativos y legales. Producto de este acompañamiento deberán generarse registros y documentos que soporten la ejecución del SIG.

3.3.1 Fase de verificación y validación

El concepto de verificación y validación surgen como etapas relevantes en los procesos de diseño e implementación, por lo cual es apropiado para la ejecución del presente proyecto de consultoría; en el marco del presente trabajo ambos momentos tienen igual aplicación. Por su parte, las actividades de seguimiento, medición, análisis y evaluación de los procesos están orientados a establecer el nivel de cumplimiento de una norma específica basado en evidencia objetiva sobre la cual se emiten una serie de hallazgos que validad la conformidad o grado de

cumplimiento de los mismos. En esta etapa vuelve a tomar relevancia la alta dirección de EXTRUCOL S.A. pues por requisitos de los sistemas de gestión en mención a integrar requieren que el seguimiento sea una entrada de información para los directivos de las organizaciones no solo para conocer el estado de las actividades sino sirva de insumo para la toma de decisiones.

Como actividad clave de validación se propone la ejecución de una auditoría interna con alcance al proceso de TI, que permita concluir la eficacia, conveniencia y adecuación del SIG.

3.4.1 Fase de mejora

La mejora continua es una de las etapas que más cobra valor quizá no en la implementación pero si en el mantenimiento y permanencia de los sistemas de gestión, además genera una ruta para definir planes de trabajo sobre los hallazgos a modo de no conformidad, oportunidades de mejora detectados en auditorias y a darle respuesta a las quejas de los clientes o partes interesadas con el fin de promover una cultura de análisis constante para mejorar y optimizar los procesos de la empresa para cumplir satisfactoriamente con los objetivos organizacionales.

4. Resultados

4.1 Acerca del objetivo específico 1, identificar el funcionamiento del área TI a través de una caracterización de procesos prioritarios, que establezca el nivel de madurez en la implementación de la norma NTC ISO/IEC 27001:2022

Un documento que ha cobrado importancia para los sistemas de gestión es la llamada caracterización de procesos, si bien ninguna norma aplicable a Extrucol S.A. exige su implementación, es una metodología utilizada para comprender la razón por la cual un proceso ha sido creado pues incluye entre otras cosas su alcance, las actividades que se realizan incluidas sus interacciones con los demás procesos de la organización, se determinan responsables y la forma como se controla para el cumplimiento de los objetivos.

Al realizar un diagnóstico inicial sobre el documento de caracterización existente S14 “caracterización proceso sistemas” en su versión 4; se evidencia que el documento no cumple con el alcance requerido según las actividades del sistema de gestión de seguridad de la información NTC ISO/IEC 27001:2022, pues su alcance está limitado a ofrecer un soporte oportuno a todos los usuarios en cuanto a requerimientos informáticos, el cual no va más allá de solucionar un inconveniente o una necesidad cuando exista.

Por lo tanto se conforma un grupo de trabajo entre los autores del presente proyecto y los ingenieros del proceso TICS, los cuales por su experiencia y conocimiento pueden ayudar a reformular la caracterización del proceso, describiendo todas las actividades que realmente se realizan y la forma como son controladas por la organización, la jefe de laboratorio y sistemas de gestión quien ayuda a orientar la metodología del manejo de la información para orientar la nueva caracterización y que esta cumpla según lo descrito en el procedimiento interno CG01 “manuales,

procedimientos, documentos y registros del sistema integrado de gestión".

Para obtener el entregable del primer objetivo se indaga a los jefes del proceso, en busca de sus ideas, conceptos, percepción sobre cada uno de los espacios a diligenciar, posterior con la experiencia de los maestrandos se ayuda a construir la caracterización S14 en una nueva versión 5, de tal forma que abarque el alcance y las actividades reales del proceso, en la cual se le da mayor relevancia a la seguridad de la información a través de las actividades realizadas en el proceso.

Tabla 3. *Caracterización proceso TI*

Caracterización proceso						
Objetivo del proceso:						**Responsable:**
Desarrollar los softwares de la empresa de tal forma que sean adecuados a las necesidades de la compañía, Ofrecer soporte oportuno a las necesidades tecnológicas y de comunicaciones; garantizar la seguridad, confidencialidad y disponibilidad de la información de la empresa.						Jefe de sistemas
Alcance:	Inicia:	Solicitud o identificación de una necesidad de equipos, soporte o desarrollo tecnológico.				
	Termina:	Entregable realizado a las necesidades o actividades del proceso.				
Interacción con otros procesos:						
Proceso emisor	**Entrada**		**Actividades**	**Responsable**	**Salida**	**Proceso receptor**
Gestión financiera	Solicitud de presupuesto anual	**P**	1. Planear y presupuestar los recursos del área.	Jefe de sistemas	Presupuesto anual	Gestión financiera
Todos los procesos	Documento Gestión de riesgos CG10. Fuentes del riesgo		2. Identificar los riesgos del proceso	Jefe de sistemas	Matriz de riesgos CG10F01	TICS
Todos los procesos	Correo electrónico		3. Recibir la solicitud o identificar una necesidad.	Coordinador de sistemas	Respuesta formal vía correo electrónico	Todos los procesos
Todos los procesos	Necesidad identificada		4. Planear la prestación del servicio.	Coordinador de sistemas	Plan de actividades	Todos los procesos
Todos los procesos	Documento gestión de riesgos CG10. fuentes del riesgo		5. Gestionar los riesgos del proceso	Jefe de sistemas	Matriz de riesgos CG10F01	TICS

Caracterización proceso						
Todos los procesos	Necesidad identificada	**H**	6. Realizar soporte técnico de equipos e información.	Coordinador de sistemas	Revisión de eventos o fallas AM09F01	Todos los procesos
Todos los procesos	Necesidad identificada		7. Realizar los desarrollos de software que se requieran.	Jefe de sistemas	Puesta en marcha de los desarrollos	Todos los procesos
Todos los procesos	Necesidad identificada	**H**	8. Realizar mantenimiento a los equipos de cómputo, cámaras de seguridad y sistemas de alarmas.	Coordinador de sistemas	Mantenimiento CCTV AM30F01	Todos los procesos
Todos los procesos	Manuales de softwares		9. Administrar los sistemas de información.	Jefe de sistemas	Operación normal de los softwares	TICS
Todos los procesos	equipos adquiridos		10. Elaborar y actualizar el inventario tecnológico	Aux de sistemas	Hoja de vida de equipos de cómputo AM06F02 Acta de entrega de equipos tecnológicos.	TICS
Todos los procesos	Necesidades de los procesos softwares adquiridos por la compañía		11. Garantizar la seguridad y servicios informáticos.	Jefe de sistemas	Formato restauración de back up AM23F01	Todos los procesos
Seguridad física	Lineamientos de la empresa	**V**	12. Monitorear las cámaras de vigilancia instaladas.	Aux de sistemas	Informe de actividades sospechosas	Seguridad física
Mejora continua	Sistemas de gestión		13. Mantener actualizados los indicadores del proceso.	Coordinador de sistemas	Socialización en comité de área	Responsabilidad gerencial. Mejora continua.

Caracterización proceso						
Mejora continua.	CG03 "Acciones correctivas y preventivas"	**A**	14. Aplicar acciones para el mejoramiento continuo; aquellas identificadas como hallazgos de auditorías o desviaciones de los indicadores.	Coordinador de sistemas	CG03F04 "Análisis de acciones correctivas, preventivas y análisis de causas" C08F01 "Acción de mejora"	Responsabilidad gerencial. Mejora continua.

Requisitos asociados		
Normas técnicas de calidad		**Legales y de la organización**
NTC ISO 9001:2015	7.5.3 control de la información documentada	No aplica.
NTC ISO 14001:2015	7.5.3 control de la información documentada	
NTC ISO/IEC 27001:2022	Todos los requisitos de la norma ISO/IEC 27011:2022.	

Documentos asociados		
Documentos	AF10	Jefe de sistemas
	AF41	Coordinador de sistemas
	AF73	Auxiliar de sistemas
	AM06	Políticas generales sobre el uso de sistemas y tecnologías de la información
	AM09	Plan de contingencia de tecnologías de la información
	AM11	Procedimiento de conversión de datos
	AM12	Creación y administración de usuarios para el uso del sistema de información oracle
	AM13	Asignación y control de claves del administrador de oracle
	AM14	Modificación al sistema de información por requerimientos de usuarios
	AM23	Procedimiento de respaldo de backup y restauración
	AM25	Procedimiento de mantenimiento y actualización de la página web
	AM26	Instalación, administración y manejo de antivirus
	AM27	Administración y evaluación de la plataforma tecnológica
	AM29	Política de seguridad de la información en servidor de archivos
	AM30	Procedimiento circuito cerrado de televisión. (cctv)
Registros		
	AM06F01	Acta de entrega y devolución de equipos de computo
	AM06F02	Hoja de vida de equipos de cómputo
	AM06F03	Acta de entrega de equipos tecnológicos
	AM06F04	Listado de autorización de salida de equipos de computo
	AM09F01	Revisión de eventos o fallas
	AM09F02	Plan de pruebas contingencias de ti
	AM12F01	Solicitud de creación de usuarios
	AM13F01	Formato asignación de clave administrador oracle (system y sys)
	AM23F01	Formato restauración de backup
	AM29F01	Manejo de información y backup por áreas del servidor de archivos
	AM30F01	Mantenimiento de cctv

Caracterización proceso	
Riesgos	Documentado en: Matriz de riesgos CG10F01.

4.2 Acerca del objetivo específico 2, definir los elementos para el diseño del Sistema de Gestión de la información a través de la metodología de requisitos comunes de las normas técnicas, de modo que se asegure la integración

La integración de los sistemas de gestión es una opción viable gracias a la estructura de alto nivel que ahora manejan las normas de los sistemas de gestión, para ello se puede hacer uso de herramientas como en este caso la metodología de requisitos comunes, en la cual basados en la integración de las normas ISO 9001:2015 e ISO 14001:2015 con la que ya cuenta la empresa EXTRUCOL S.A, se definieron los numerales de la norma NTC ISO/IEC 27001:2022 que coincidían con los de las normas previamente mencionadas tabulándolas en una lista de chequeo. Posteriormente se procede a definir los documentos con que la empresa da cumplimiento a los requisitos de cada sistema de gestión y se analiza a qué proceso pertenece, definiendo el porcentaje de cumplimiento al momento de realizar el diagnóstico que presenta relacionado a la integración de la norma de seguridad de la información utilizando una tabla de colores que especifica dicho porcentaje.

Tabla 4. *Listado maestro de documentos proceso TI*

Proceso	Código	Titulo documento	Plantilla
TI	AM06F03	Acta de entrega de equipos tecnológicos	Formato
TI	AM06F01	Acta de entrega y devolución de equipos de computo	Formato
TI	AM27	Administración y evaluación de la plataforma tecnológica	Procedimiento
TI	AM13	Asignación y control de claves del administrador de Oracle	Procedimiento
TI	AF73	Auxiliar de ti	Perfil de cargo
TI	AM12	Creación y administración de usuarios para el uso de los sistemas de información	Procedimiento
TI	AM13F01	Formato asignación de clave administrador Oracle (system y sys)	Formato

Proceso	Código	Titulo documento	Plantilla
TI	AM23F01	Formato restauración de backup	Formato
TI	AM06F02	Hoja de vida de equipos de cómputo	Formato
TI	AM26	Instalación, administración y manejo de antivirus	Procedimiento
TI	AM06F04	Listado de autorización de salida de equipos de computo	Formato
TI	AM29F01	Manejo de información y backup por áreas del servidor de archivos	Formato
TI	AM30F01	Mantenimiento de CCTV	Formato
TI	AM14	Modificación al sistema de información por requerimientos de usuarios	Procedimiento
TI	AM09	Plan de contingencia de tecnologías de la información	Procedimiento
TI	AM09F02	Plan de pruebas contingencias de ti	Formato
TI	AM06	Política de recursos tecnológicos y sistemas de información	Procedimiento
TI	AM29	Política de seguridad de la información en servidor de archivos	Procedimiento
TI	AM28	Política de uso de dispositivos de almacén, amiento externo y/o medios extraíbles.	Procedimiento
TI	AM30	Procedimiento circuito cerrado de televisión. (CCTV)	Procedimiento
TI	AM11	Procedimiento de conversión de datos	Procedimiento
TI	AM25	Procedimiento de mantenimiento y actualización de la página web	Procedimiento
TI	AM23	Procedimiento de respaldo de backup y restauración	Procedimiento
TI	AM09F01	Revisión de eventos o fallas	Formato
TI	S14	Caracterización proceso ti	Caracterización
TI	AM12F01	Solicitud de creación de usuarios	Formato
PLANIF. SIG	C01F03	Acta de revisión por la dirección	Formato
PLANIF. SIG	CG16	Análisis del contexto interno y externo de la organización	Procedimiento
PLANIF. SIG	C04F11	Análisis DOFA	Formato
PLANIF. SIG	C04F09	Análisis externo PESTAL	Formato
PLANIF. SIG	C04F10	Análisis interno	Formato
PLANIF. SIG	CG10	Gestión de riesgos	Procedimiento
PLANIF. SIG	CG05F01	Gestión del cambio	Formato
PLANIF. SIG	PG01	Manual del sistema integrado de gestión	Manual
PLANIF. SIG	CG08	Mapa de procesos	Mapa de procesos
PLANIF. SIG	C04F29	Matriz de comunicaciones	Formato
PLANIF. SIG	CG10F01	Matriz de riesgos	Formato

Proceso	Código	Titulo documento	Plantilla
PLANIF. SIG	C04F14	Necesidades y expectativas de las partes interesadas	Formato
PLANIF. SIG	C04F13	Oportunidades	Formato
PLANIF. SIG	C04F08	Planificación estratégica de gestión especificación de los recursos del plan estratégico de gestión	Formato
PLANIF. SIG	C01F08	Plantilla revisión del sistema	Formato

Finalmente se definen los cambios correspondientes que se deben realizar en cada documento y los respectivos responsables de dicho proceso, teniendo en cuenta que debe ser personal de la empresa quienes aprueben las modificaciones propuestas en el presente proyecto de grado que busca integrar la norma NTC ISO/IEC 27001:2022 con las demás ya implementadas en la compañía.

Adjunto al presente documento, se muestra la matriz que define la integración de la norma NTC ISO/IEC 27001:2022 con las normas ya implementadas en la empresa como son ISO 9001:2015 e ISO 14001:2015. (Ver apéndice B)

4.3 Acerca del objetivo específico 3, implementar el Sistema de Gestión de la información a través del acompañamiento en la ejecución de los lineamientos documentados, de manera que se asegure su asimilación en área TI

La implementación de un sistema de gestión en una estructura de alto nivel debe tener en cuenta los documentos creados y los procedimientos correspondientes a la norma aplicable en el contexto específico del área de Tecnologías de la Información (TI) se busca salvaguardar la información de manera efectiva mediante diversos procedimientos y políticas que aplican desde el personal interno de la compañía hasta los entes externos que puedan llegar a tener acceso a la información de la empresa.

La empresa cuenta con documentos específicos donde se consigna información transversal en la compañía, se estipulan procedimientos, perfiles de cargo, políticas, se relacionan formatos, planes de contingencia, reglamento para el uso de los elementos de la compañía, roles y responsabilidades de las partes interesadas, información pública de la compañía relacionada al contexto entre otros. También se cuenta con diversos formatos que permiten diligenciar desde actividades rutinarias, hasta procesos de contingencia, recepción de equipos, planes de mantenimiento, etc.

Para la implementación de la norma NTC ISO/IEC 27001:2022 los investigadores se apoyaron en la matriz de diagnóstico preliminar donde se proporcionan los datos relacionados a los procesos que no cumplen con la exigencia de la norma, por ende, se procede a revisar los documentos de la compañía aplicables a cada numeral, estos documentos abordan una variedad de aspectos cruciales, desde la definición de roles y responsabilidades de las partes interesadas hasta la regulación del uso de los recursos de la compañía; se relacionan y en caso de requerir modificaciones, se realizan o se crean nuevos documentos o formatos, al considerar los documentos creados y los procedimientos correspondientes, se garantiza una sólida estructura para identificar, evaluar y mitigar los riesgos de seguridad de la información cabe resaltar que la implementación se realizó a cabalidad y se evidencia en el desarrollo del siguiente objetivo con la auditoría por parte del personal capacitado de la compañía.

En los requisitos relacionados al “planear” de la norma NTC ISO/IEC 27001:2022 se implementó partiendo de la comunicación con la alta dirección, el personal responsable del proceso y personal a cargo de los sistemas integrados de gestión. Se definió un plan de trabajo acorde con la metodología propuesta de implementar la NTC ISO/IEC 27001:2022 por medio de los requisitos comunes compartidos con las normas NTC ISO 9001:2015 Y NTC ISO 14001:2015.

Posterior se modificaron los formatos donde se analiza el contexto de la organización y agregando los factores que a través del tiempo han venido afectando el entorno, como lo ha sido los últimos años el aumento de los ataques cibernéticos a las grandes empresas a raíz de descuidos de los colaboradores en sus dispositivos de trabajo, recepción de correos maliciosos, pérdida de documentos importantes para la compañía entre otros riesgos que evitan el cumplimiento de las necesidades y expectativas de las partes interesadas así como, basados en el diagnóstico inicial realizado. Adicional se actualizan registros como matriz de comunicaciones, matriz de necesidades y expectativas de las partes interesadas, se rediseña la caracterización del proceso de TI, los perfiles de cargo del personal y se documenta la política del proceso acorde a lo requerido.

Tabla 5. *Matriz de requisitos aplicados al sistema de gestión integral (planificar)*

Matriz de requisitos aplicados al sistema de gestión integral de Extrucol S.A

Fecha de actualización 02/09/2023	Realizado por:	David Arias /Henry Albarracín	Requisito Aplicable para ISO 9001:2015, ISO 14001:2015 e ISO/IEC 27001:2022	Valoraciones	
Requisitos de la norma **ISO/IEC 27001:2022**			**Descripción aplicación de los requisitos**	**Según diagnóstico**	**Posterior a la implementación**
Capítulo planear					
4. Contexto de la organización					
4.1 Comprensión de la organización y de su contexto			Se cuenta con matriz PESTAL código C04F09 para el análisis externo y matriz DOFA código C05F10 para análisis interno	**25%**	**100%**
4.2 Comprensión de las necesidades y expectativas de las de otras partes interesadas			Se encuentra con el documento código C04F14 que corresponde a "Necesidades y expectativas de las partes interesadas"	**25%**	**100%**

Matriz de requisitos aplicados al sistema de gestión integral de Extrucol S.A			
4.3 Determinación del alcance del sistema de gestión de la seguridad de la información	Se encuentra definido en el "manual de tecnologías de la información código AM00"	**25%**	**100%**
4.4 Sistema de gestión de la seguridad de la información	caracterización S14 "Sistemas"	**25%**	**100%**
Capítulo planear	------		
5. Liderazgo (título)	------		
5.1 Liderazgo y compromiso	Se cuenta con un presupuesto asignado al área de TI para una ejecución anual. Se cuenta con un plan anual de capacitación consignado en el formato "CG02F14" donde se consignan capacitaciones para ejecución anual acerca de la seguridad de la información.	**0%**	**100%**
5.2 Política seguridad de la información	Se cuenta consignada el procedimiento AM06 "política de recursos tecnológicos y seguridad de la información"	**50%**	**100%**
5.3 Roles, responsabilidades y autoridades en la organización	Perfiles de cargo AF73 "auxiliar de sistemas", AF41 "coordinador de sistemas", AF10 "jefe de sistemas"	**75%**	**100%**
Capítulo planear	------		
6. Planificación (título)	------		
6.1 Acciones para abordar riesgos y oportunidades 6.1.1 Generalidades 6.1.2 Valoración de los riesgos de la seguridad de la información 6.1.3. Tratamiento de los riesgos de la seguridad de la información	Cuenta con el procedimiento interno CG10 "gestión de riesgos" y adicional con la matriz de riesgos CG10F01 Está pendiente incluir en el procedimiento la matriz de declaración de aplicabilidad, y relacionar el sistema de gestión de seguridad de la información en el alcance.	**75%**	

Matriz de requisitos aplicados al sistema de gestión integral de Extrucol S.A

6.2 Objetivos de seguridad de la información y planificación para lograrlos	En todos los procedimientos del sistema de gestión, se encuentran relacionados diferentes objetivos que aportan al fortalecimiento del sistema.	**75%**	**100%**

El capítulo relacionado con el "hacer" es el más extenso pero clave, debido al manejo de controles y operaciones que se realizan a nivel de seguridad de la información desde el momento que se ingresa a la compañía, hasta los procesos relacionados al manejo del software, antivirus y demás elementos que influyen en la realización de las labores rutinarias de los colaboradores, visitantes, contratistas y demás

Es en esta etapa donde se intensificaron las reuniones con el personal de TI, para documentar aquellas prácticas o controles establecidos y se tuvo en cuenta el personal de SGI para que todos los procedimientos quedaran acordes con lo requerido en el manual CG01 "Manuales - Procedimientos - Documentos y registros del sistema integrado de gestión".

Se utilizaron entrevistas concertadas con anticipación, llamadas telefónicas, videoconferencias, de tal forma de no limitar únicamente a entrevistas presenciales, dado que Extrucol S.A. maneja días de trabajo en casa y la intención siempre fué no dilatar los tiempos de trabajo. En dichos espacios de trabajo, se realizaban anotaciones tipo borrador para posteriormente documentar la información recibida para que posteriormente, fuese puesto a revisión del ingeniero de TI.

Es imperativo resaltar que, en este capítulo, quizá lo que más tiempo demandó fue documentar los controles requeridos por la norma NTC ISO 27001:2022, en su anexo A, los cuales son considerados los pilares fundamentales del sistema implementado. Para ello se construyó un

documento desde cero, que para practicidad de la organización se describieron uno a uno los controles requeridos y aquellos que ya se encontraban en otro registro o procedimiento se relacionaron en el manual indicando claramente el código y nombre con el fin de evitar la duplicidad de información y que, en futuras actualizaciones, se disminuya el riesgo de tener documentos con diferente contenido al modificar uno y olvidar actualizar los demás.

Tabla 6. *Matriz de requisitos aplicados al sistema de gestión integral (Hacer)*

Matriz de requisitos aplicados al sistema de gestión integral de Extrucol SA

echa de actualización: 02/09/2023	Realizado por:	David Fabián Arias/Henry Alexander Albarracín	Requisito Aplicable para ISO 9001:2015, ISO 14001:2015 e ISO/IEC 27001:2022	Valoraciones	
Requisitos de la norma ISO/IEC 27001:2022			**Descripción aplicación de los requisitos**	**Según diagnóstico**	**Posterior a la implementación**
Capítulo hacer					
7.Soporte (Título)					
7.1 Recursos			Se lleva control en la ejecución del presupuesto anual.	**75%**	**100%**
7.2 Competencia			Perfiles de cargo AF73 "auxiliar de sistemas", AF41 "coordinador de sistemas", AF10 "jefe de sistemas" en las hojas de vida del personal se encuentran los soportes de la competencia del personal a cargo de seguridad de la información.	**75%**	**100%**
7.3 Toma de Conciencia			no requiere documento, se valida con el conocimiento de los controles establecidos en la organización por parte de los colaboradores.	**25%**	**100%**
7.4 Comunicación			matriz de comunicaciones C04F29 Se actualiza incluyendo nuevas necesidades de comunicación acordes con el sistema de gestión de seguridad de la información.	**50%**	**100%**

Matriz de requisitos aplicados al sistema de gestión integral de Extrucol SA			
7.5 Información Documentada 7.5.1 Generalidades 7.5.2 Creación y actualización 7.5.3 Control de la información documentada	procedimiento CG01 "manuales - procedimientos - documentos y registros del sistema integrado de gestión"	**50%**	**100%**
Capítulo hacer			
8. Operación (Título)			
8.1 Planificación y Control Operacional	AM00 manual de tecnologías de la información af73 auxiliar de sistemas AM06 políticas generales sobre el uso de sistemas y tecnologías de la información AM06f01 acta de entrega y devolución de equipos de cómputo AM06f02 hoja de vida de equipos de cómputo AM06f03 acta de entrega de equipos tecnológicos AM06f04 listado de autorización de salida de equipos de cómputo AM09 plan de contingencia de tecnologías de la información AM09f01 revisión de eventos o fallas AM09f02 plan de pruebas contingencias de ti AM11 procedimiento de conversión de datos AM12 creación y administración de usuarios para el uso del sistema de información Oracle AM12f01 solicitud de creación de usuarios AM13 asignación y control de claves del administrador de Oracle AM13f01 formato asignación de clave administrador Oracle (system y sys) AM14 modificación al sistema de información por requerimientos de usuarios AM23 procedimiento de respaldo de backup y	**25%**	**100%**

Matriz de requisitos aplicados al sistema de gestión integral de Extrucol SA

	restauración AM23f01 formato restauración de backup AM25 procedimiento de mantenimiento y actualización de la página web AM26 instalación, administración y manejo de antivirus AM27 administración y evaluación de la plataforma tecnológica AM29 política de seguridad de la información en servidor de archivos AM29f01 manejo de información y backup por áreas del servidor de archivos AM30 procedimiento circuito cerrado de televisión. (cctv) AM30f01 mantenimiento de cctv S14 sistemas CG05 planificación de cambios del sistema integrado de gestión"		
8.2 Valoración de los riesgos de la seguridad de la información	Se cuenta con el procedimiento interno CG10 "gestión de riesgos" y adicional con la matriz de riesgos CG10F01	**75%**	**100%**
8.3 Tratamiento de los riesgos de la seguridad de la información	Se cuenta con el procedimiento interno CG10 "gestión de riesgos" y adicional con la matriz de riesgos CG10F01	**75%**	**100%**

El capítulo relacionado al "verificar", se rediseñaron indicadores en pro de realizar seguimiento a los controles implementados en los diferentes procesos relacionados al área de TI, también, se ejecutó una auditoría interna al proceso de TI, la cual fue realizada por un ingeniero de sistemas, especialista en seguridad informática y actual estudiante de maestría en administración de tecnologías de la información, la cual arroja un balance positivo de la implementación del presente trabajo de grado.

Para la auditoría realizada, se cuenta con evidencias como plan de auditoría y su correspondiente informe (Ver apéndice C).

Se modificó el formato de modelo de revisión por la dirección, para que, en futuras reuniones, se tengan en cuenta las entradas y salidas descritas en la norma NTC ISO/IEC 27001:2022.

Tabla 7. *Matriz de requisitos aplicados al sistema de gestión integral (verificar)*

Matriz de requisitos aplicados al sistema de gestión integral de Extrucol S.A.

Fecha de actualización: 02/09/2023	Realizado por:	David Arias/Henry Albarracín	Requisito Aplicable para ISO 9001:2015, ISO 14001:2015 e ISO/IEC 27001:2022	Valoraciones	
Requisitos de la norma ISO/IEC 27001:2022			Descripción aplicación de los requisitos	Según diagnóstico	Posterior a la implementación
Capítulo verificar					
9. Evaluación del Desempeño (Título)					
9.1 Seguimiento, Medición, Análisis y Evaluación del Desempeño			Se evidencian indicadores del proceso plasmados en el dashboard manejado por la analista de planeación financiera. Se propone la adición o cambios de indicadores.	50%	100%
9.2 Auditoría Interna			"CG04 Auditorías internas de los sistemas de gestión", "CG04F03 Programa de auditorías/Revisión por la dirección", "CG04F09 Plan de auditorías internas", "CG04-A2 Perfil y competencias de los auditores", "CG04F10 Selección de auditores (Calificación)". Se incluye dentro del alcance del procedimiento y el anexo el sistema de gestión NTC ISO/IEC 27001:2022.	0%	100%
9.3 Revisión por la Dirección			"C01F03 " Acta de revisión por la dirección. Pendiente realizar la revisión por la dirección.	0%	

Finalmente, en el proceso de "actuar", se busca la mejora continua del sistema de gestión, se revisa si el proceso de TI cuenta con no conformidades que provengan de auditorías previas; las cuales no se evidencian en el proceso en la ejecución de la auditoría realizada (ver apéndice C).

Tabla 8. *Matriz de requisitos aplicados al sistema de gestión integral (Actuar)*

Matriz de requisitos aplicados al sistema de gestión integral de Extrucol S.A.

Fecha de actualización: 02/09/2023	Realizado por:	David Arias/Henry Albarracín	Requisito Aplicable para ISO 9001:2015, ISO 14001:2015 e ISO/IEC 27001:2022	Valoraciones	
Requisitos de la norma ISO/IEC 27001:2022			Descripción aplicación de los requisitos	Según diagnóstico	Posterior a la implementación
Capítulo actuar					
10. Mejora (Título)					
10.1 NO Conformidades y Acciones Correctivas			"CG03 Acciones correctivas"	75%	100%
10.2 Mejora Continua			"C08F01 Acción de mejora", "C08F02 Seguimiento acciones de mejora"	75%	100%

La norma NTC ISO/IEC 27001:2022 tiene un punto clave que se debe tratar y son los controles implementados según las clasificaciones que nos proporcionan, en el caso de la empresa Extrucol SA, se revisó cada uno de los puntos que sugiere la norma y posteriormente analizando los documentos de la compañía que especifican los controles aplicables y en caso de no ser necesarios, se especifican las razones. La normativa hace énfasis en los controles que se efectúan para mitigar evitar la materialización de los riesgos presentes en el área de TI, bajo la guía del jefe de sistemas, se procede a revisar detalladamente el control y en caso de estar presente, se documenta, pero en los casos donde no se cuenta con los controles respectivos, se implementan

por medio de revisiones personales, instalación de equipos de vigilancia, el uso de software específico para el manejo de la información, uso de cuentas empresariales con usuarios y contraseñas directas con exigencias de seguridad, tiempos de bloqueo según periodos de inactividad, la prohibición de dispositivos externos y peligrosos para mover información, realización de copias de seguridad por parte del sistema, manejo de sistemas de antivirus licenciados y vigilados constantemente, aplicación de guías para el cuidado de dispositivos de la compañía entre otros controles basados en la exigencia que aborda la norma.

4.4 Acerca del objetivo específico 4, Evaluar el cumplimiento de los requisitos de la norma NTC ISO/IEC 27001:2022 en el área TI de la empresa Extrucol, a través de un proceso de una auditoría interna que determine la conformidad del sistema de gestión.

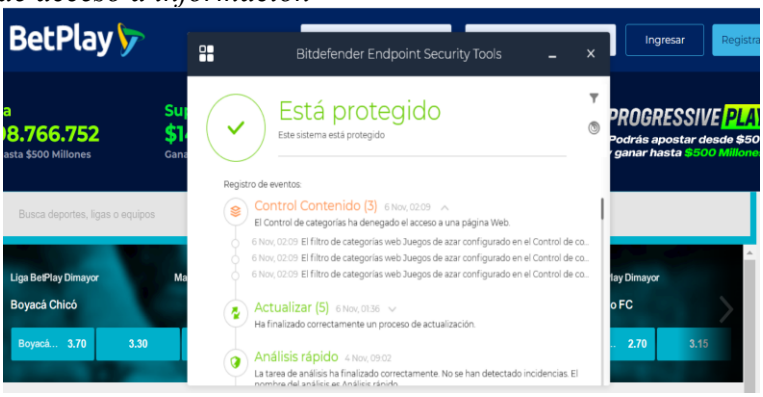
Es importante resaltar que no se puede adjuntar documentos o registros, pues se consideran propiedad intelectual de la empresa y no está permitido su divulgación a terceros.

Sin embargo, con el fin de evidenciar que se tienen controles establecidos para cumplir con los requisitos del sistema de gestión de seguridad de la información se describen los siguientes:

En el proceso TI, se tienen controles que no permiten:

- Correos electrónicos personales (Excepción Gmail)
- Páginas de Juegos en línea.
- Páginas de descarga de aplicaciones
- Redes sociales
- Paginas explicitas de adultos
- Paginas con material explícito o violento
- Páginas de almacenamiento en la nube (Excepción Google Drive)

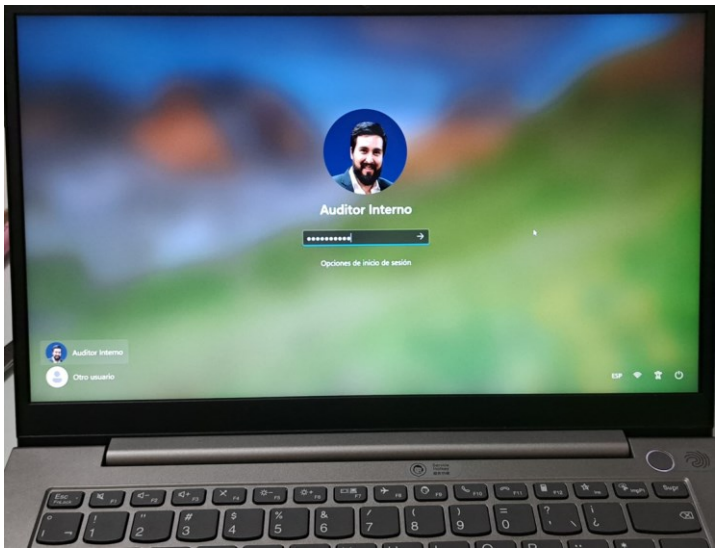
Figura 6. *Control de acceso a información*



Nota. La figura muestra la efectividad de los controles establecidos.

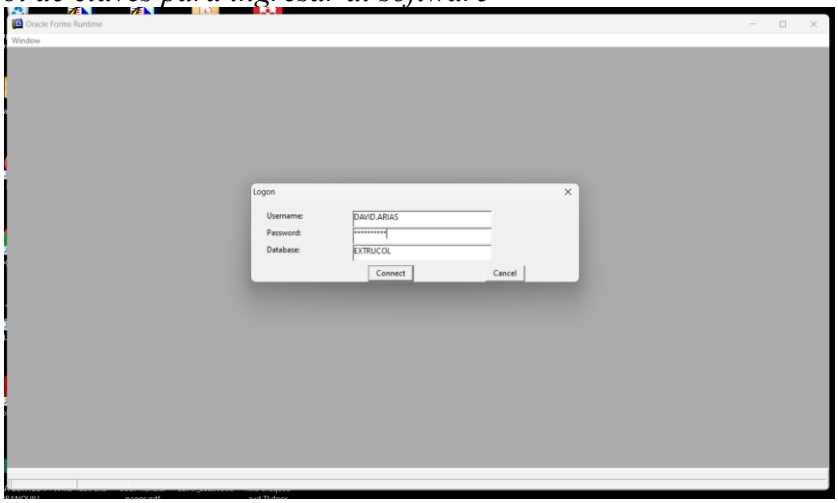
Control de claves que requiere contraseña con vencimiento cada 3 meses y debe contener como mínimo: una mayúscula, una minúscula, un número y un carácter.

Figura 7. *Control de claves de acceso*



Nota. La figura muestra la necesidad de ingresar una contraseña para iniciar.

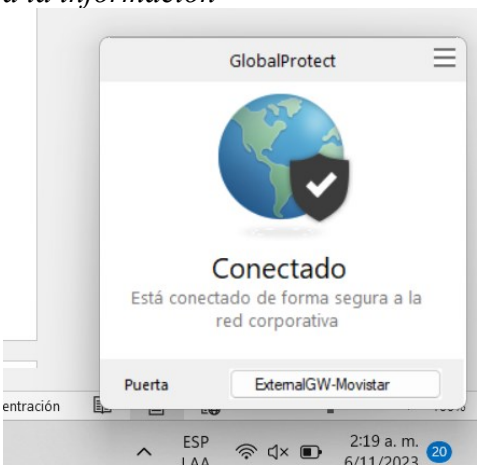
Figura 8. *Control de claves para ingresar al software*



Nota. La figura muestra la necesidad de ingresar una contraseña para acceder al software.

La empresa cuenta con un túnel seguro con políticas precisas para restringir o autorizar el acceso según la necesidad empresarial.

Figura 9. *Software de acceso a la información*



Nota. La figura muestra la conexión a software que garantiza acceso seguro a la información.

Se solicita vía correo electrónico incluir en el plan de capacitación del personal, información acerca de la seguridad del proceso TI y queda programada para el mes de noviembre.

Figura 10. *Solicitud de capacitación para el personal*

Hola Sharol, espero estés bien,

Porfa coordina con Willian Camacho para que puedas agendar una capacitación ya el te mencionará si a todo el personal o solo administración

Tema: tipos de ciberataques. Y esta la puedes catalogar como capacitación BASC.

El ya sabe del tema, ya lo conversamos, es solo que te confirme en qué fecha.

Cordialmente,

DAVID FABIAN ARIAS CAÑAS
AUDITOR INTERNO

EXTRUCOL
REDES CONFIABLES

Parque Industrial I Km. 3 Vía Palenque Café Madrid.
Bucaramanga – Colombia, South América
Celular: (+57) 3162205288
auditoriainterna@extrucol.com

Nota. La figura muestra la solicitud realizada para fortalecer las competencias del personal.

Con el fin de dar cumplimiento al objetivo 4, se realiza una auditoría posterior a la implementación total del sistema de gestión NTC ISO/IEC 27001:2022 (ver apéndice C), ya que basados en la metodología PHVA se debe obtener una retribución por parte de personal capacitado, que nos brinde una retroalimentación al trabajo realizado y de esta manera, mantener el mejoramiento continuo del sistema por parte de la empresa en aras de buscar una certificación al mismo en un futuro.

La persona encargada de realizar la auditoría es el ingeniero Willian Camacho Pinto quien cumple con las competencias descritas en el procedimiento interno de selección de auditores y cuenta con las competencias para ejecutar auditorías bajo el esquema de la NTC ISO/IEC 27001.

En dicho informe de auditoría se concluye “se considera que el proceso de TI cuenta con la documentación en la extensión necesaria y los controles establecidos para cumplir con lo requerido en la NTC ISO 27001:2022 y se encuentra alineada al sistema integrado de gestión de la empresa que incluye NTC ISO 9001:2015 y NTC ISO 14001:2015.”

5. Discusión

Extrucol SA es una empresa comprometida con la seguridad de la información tanto dentro como fuera de la compañía, generando conciencia en los colaboradores y en todo el personal para que se cuide el recurso más valioso como es la información. Para esto, se implementaron controles para las diferentes áreas de la compañía que pueden correr riesgo de vulnerabilidad desde los más básicos, hasta las áreas fundamentales. Se procede a concienciar al personal de la empresa desde el manejo de dispositivos electrónicos, accesos a correos electrónicos, la exposición de información en los escritorios y áreas comunes a personal no autorizado, el uso de equipos corporativos, cuidado, mantenimiento y disposición final del mismo, también se evidencia la capacidad del personal y sus respectivas funciones desde el manual teniendo en cuenta la responsabilidad en cuanto a seguridad de la información entre más controles que permiten un manejo de la información de forma segura. Se presentaron inconvenientes en algunos documentos que no especifican ciertos controles que sí se desarrollaban, pero no se documentaron, también se presentaron retrasos en la facilidad de la información debido a factores externos que se presentaron, pero al final se logró la adquisición de ciertos documentos importantes para el desarrollo total del proyecto. Es fundamental la correcta documentación de los procesos, ya que mantener una comunicación lo más clara posible permite un mejor desarrollo de actividades y que todo el personal entienda los riesgos y cuidados a los que están expuestos.

6. Conclusiones

La constancia y el trabajo en equipo tanto de Extrucol S.A., como de los maestrandos y el director de la tesis, fueron determinantes para la consecución con cada uno de los objetivos trazados y cumplirlos todos a cabalidad.

La caracterización del proceso de TI, permitió identificar el nivel de cumplimiento de los requisitos de la norma NTC ISO/IEC 27001:2022. Las mejoras y ajustes realizados durante la implementación han contribuido significativamente al aumento de la madurez en los procesos de seguridad de la información. Esto se traduce en una mayor capacidad para prevenir, detectar y responder a amenazas y vulnerabilidades.

La metodología de requisitos comunes de las normas técnicas facilitó el diseño del Sistema de Gestión de la Información de manera integrada con las normas ISO 9001:2015 y ISO 14001:2015. Esta integración proporciona coherencia y consistencia en los procesos organizativos, generando eficiencias operativas y cumpliendo con los estándares de calidad y gestión ambiental.

La implementación del SGSI planteada en el tercer objetivo específico, no solo fortalece la postura de seguridad de la información, sino que también genera valor para las partes interesadas, incluidos clientes, socios comerciales y reguladores. La transparencia y la seguridad de los procesos de TI mejoran la confianza en Extrucol como entidad comprometida con la protección de la información y el cumplimiento normativo.

La ejecución del presente proyecto ha permitido a Extrucol identificar y evaluar los riesgos de seguridad de la información a los que está expuesta, así como implementar controles para mitigarlos. Esto ha contribuido a reducir la probabilidad y el impacto de los incidentes de seguridad de la información.

Posterior a la pandemia vivida, la virtualidad y trabajo remoto se ha vuelto muy común y con aquello el acceso a las bases de datos desde puntos externos a las instalaciones de la empresa, por ello era necesario aumentar el nivel de controles para garantizar tanto la disponibilidad como la seguridad de la información.

Es importante que todos los colaboradores de Extrucol comprendan la importancia de la seguridad de la información y sus roles y responsabilidades en la protección de la información; Extrucol debe implementar un programa de concientización y capacitación que cubra todos los aspectos del SGSI.

Se evidencia que previo a la implementación del sistema de gestión NTC ISO/IEC 27001:2022, la empresa Extrucol S.A. Cuenta con personal calificado que entiende la importancia de la información y ha implementado controles para mitigar el riesgo que se vea comprometida frente a un intento de ataque cibernético.

La auditoría interna realizada para evaluar el cumplimiento de los requisitos de la norma NTC ISO/IEC 27001:2022 evidenció la conformidad del sistema de gestión en el área de TI de Extrucol. Esto proporciona una base sólida para la certificación externa y refuerza la confianza de los stakeholders en la seguridad de la información dentro de la organización.

Referencias

Abad Peña, M. B. (2015). *Cómo gestionar la seguridad de la información (según ISO 27001: 2013) en una PYME del sector de las tecnologías de la información y la comunicación* . Valladolid : Universidad de Valladolid .

Alvarado, C. (s.f.). *Pensemos*. https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas

CAMPUSCERT. (s.f.). *CAMPUSCERT*. https://campus.certcampus.com/itil/gestion-de-proveedores/#:~:text=La%20Gesti%C3%B3n%20de%20Proveedores%20se,calidad%20a%20un%20precio%20adecuado.

Ciberseguridad. (s.f.). *Ciberseguridad*. https://ciberseguridad.com/normativa/espana/sgsi/

Extrucol S.A. (2023). Manual del sistema integrado de gestión. En Extrucol.

García, G., y Castro, J. (2017). *Repositorio Universidad Nacional Abierta y a Distancia.* https://repository.unad.edu.co/bitstream/handle/10596/11914/5685072.pdf?sequence=4yisAllowed=y

Garía, R. A. (2016). *Repositorio Universidad Abierta y a Distancia.* https://repository.unad.edu.co/bitstream/handle/10596/12722/1049605794.pdf?sequence=3yisAllowed=y

Gonzalez, J. C. (2016). *Repositorio Universidad Nacional Abierta y a Distancia.* https://repository.unad.edu.co/bitstream/handle/10596/11907/76041068.pdf?sequence=1yisAllowed=y

Gutierrez, H., y Valencia, A. (2006). *Repositorio Universidad Libre*. https://repository.unilibre.edu.co/bitstream/handle/10901/11006/CAP%C3%83%20TULO%206.pdf?sequence=10yisAllowed=y

IBM. (2021). *IBM*. https://www.ibm.com/docs/es/i/7.3?topic=security-policy-objectives

IBM. (2022). *IBM*. https://www.ibm.com/docs/es/sim/7.0.1?topic=logs-security-log-accesslog

ICONTEC. (2015). *Sistemas de Gestión Ambienta. Requisitos con orientación para su uso.* Bogotá: ICONTEC.

ICONTEC. (2015). *Sistemas de Gestión de la Calidad. Requisitos* . Bogotá: ICONTEC.

ICONTEC. (2022). *CRAI Universidad Santo Tomás seccional Bucaramanga*. https://login.crai-ustadigital.usantotomas.edu.co/login?qurl=https://ecollection.icontec.org%2fpdfview%2fviewer.aspx%3flocale%3des-CO%26Q%3d12C1D92148D1BE889D9DF275A03737C50A89E6AF43655CE9%26Req%3d

ICONTEC. (2022). *Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de Gestión de Seguridad de la información. Requisitos.* Bogotá: ICONTEC.

ICONTEC. (2023). *ICONTEC*. https://www.icontec.org/eval_conformidad/certificacion-iso-27001-sistemas-de-gestion-de-seguridad-de-la-informacion-2/

ISO. (2022). *Structure and drafting principles for International Standards. Geneva, Switzerland: ISO.* ISO.

La República. (2021). Ataques cibernéticos ocurren frecuentemente a pequeñas y medianas empresas. *La República*.

Méndez, G. E. (2020). *Propuesta mediante la normativa ISO 27001 para la gestión de la seguridad de la información en.* Heredia: Universidad Latina de Costa Rica.

Méndez, G. E. (2020). *Repositorio Universidad Latina Campus Heredia.* https://repositorio.ulatina.ac.cr/bitstream/20.500.12411/293/1/TFG_Ulatina_Gilberto_Solano_Mendez_201303104978.pdf

Monsalve, J., Aponte, F., y Chaves, D. (2014). *Revista Facultad de Ingeniería Universidad Pedagogica y Tecnológica de Colombia.* https://www.redalyc.org/pdf/4139/413937008007.pdf

Palacios Guillem, M., Perez-Bernabeu, E., y Gisbert Soler, V. (2019). *Repositorio Universidad Politécnica de Valencia*. https://3ciencias.com/wp-content/uploads/2019/05/art-1-3C-EMPRESA-ED-38-VOL-8-N-2.pdf

Peña, A., y Belén , M. (2015). *Repositorio Universidad de Valladolid.* https://core.ac.uk/download/pdf/211100419.pdf

Portafolio. (2021). Aumentan en 30% los ataques cibernéticos en Colombia. *Portafolio*.

Quispe, E. S. (2020). *Implementación de la norma ISO 27001 en el Departamento de Tecnología de Información de la empresa Esvicsac, Callao* . Lima: Universidad César Vallejo.

Quispe, E. S. (2020). *Repositorio Universidad César Vallejo.* https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/47276/Arias_QES-SD.pdf?sequence=1yisAllowed=y

Quispe, E. S. (2020). *Repositorio Universidad César Vallejo.* https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/47276/Arias_QES-SD.pdf?sequence=1yisAllowed=y

Regueros, L. A. (2023). *AUDEA*. https://www.audea.com/controles-de-seguridad-y-sus-tipos/

Rojas, M. C. (2016). *Repositorio Universidad Santo Tomás Seccional Bucaramanga.* https://repository.usta.edu.co/bitstream/handle/11634/1749/2016-CepedaRojasMariaCamila-trabajo%20de%20grado.pdf?sequence=1yisAllowed=y

Safety Culture. (2023). *Safety Culture*. https://safetyculture.com/es/temas/analisis-de-riesgos/

Sphera's Editorial Team. (2022). *SPHERA*. https://sphera.com/glosario-es/que-es-la-gestion-de-

incidentes/?lang=es

Universitat ramón llulL. (s.f.). *IQS* . https://www.iqs.edu/es/que-es-una-auditoria-y-cuales-son-sus-tecnicas