Universidad Técnica Nacional

Sede del Pacífico

Licenciatura en Ingeniería en Tecnologías de Información

Proyecto de Graduación

ANALIZAR LOS CONTROLES PARA LA SEGURIDAD DE LA INFORMACIÓN IMPLEMENTADOS POR LA EMPRESA DISTRIBUIDORA COARSA, EN SAN RAMÓN DE ALAJUELA, DE ACUERDO CON LA NORMA ISO 27002, DURANTE EL SEGUNDO SEMESTRE DEL AÑO 2022

Estudiantes

William García Molina

6 0436 0917

Michelle Rodríguez Hernández

6 0455 0898

Puntarenas, 2023

HOJA DE APROBACIÓN

En la ciudad de Puntarenas, a los 12 días del mes de agosto del año 2023 al ser las 09 horas, estando presentes en el Campus Juan Rafael Mora Porras de la Sede del Pacífico de la Universidad Técnica Nacional, las siguientes personas:

Profesor Tutor: Oberto Santín Cuesta
Profesor Lector: Roberto Escobar Agüero.
Representante del Sector Productivo: Erick Saborío Berger
Presidente del Tribunal Examinador: Antonieta González Esquivel.

En su condición de miembros del Tribunal Evaluador, para evaluar el Proyecto de Graduación para optar por el grado de **Licenciatura en Ingeniería en Tecnologías de Información**, de las personas estudiantes, **Michelle Rodríguez Hernández; William García Molina.**

Reunido el Tribunal Evaluador, los aspirantes procedieron a presentar y defender su Proyecto de Graduación titulado, **"Analizar los controles para la seguridad, de la información implementados, por la empresa distribuidora COARSA, en San Ramón de Alajuela, de acuerdo con la norma ISO- 27002, durante el segundo semestre del año 2022".**

Concluida la presentación y defensa del Proyecto de Graduación, el Tribunal Evaluador consideró que, de conformidad con la normativa en la materia, las personas estudiantes obtuvieron la **APROBACIÓN DE SU TRABAJO FINAL DE GRADUACIÓN** y les es conferido el grado de **Licenciados en Ingeniería en Tecnologías de Información.**

Oberto Santín Cuesta
Profesor Tutor

Roberto Escobar Agüero
Lector

Erick Saborío Berger
Representante del Sector Productivo

Antonieta González Esquivel
Presidente del Tribunal Examinador

Carrera Sello UTN Universidad Técnica Nacional Tecnologías de Información

Estudiantes:

Michelle Rodríguez Hernández

William García M.

William García Molina

Universidad Técnica Nacional
Ingeniería en Tecnologías de Información
Sede del Pacífico

2023 Universidades Públicas ante el Cambio Climático

ACTA DE APROBACIÓN

En la ciudad de Puntarenas, a los 12 días del mes de agosto del año 2023 al ser las 09 horas, estando presentes en el Campus Juan Rafael Mora Porras de la Sede del Pacífico de la Universidad Técnica Nacional, las siguientes personas:

Profesor Tutor: Oberto Santín Cuesta
Profesor Lector: Roberto Escobar Agüero.
Representante del Sector Productivo Erick Saborío Berger
Presidente del Tribunal Examinador: Antonieta González Esquivel.

En su condición de miembros del Tribunal Evaluador, para evaluar el Proyecto de Graduación para optar por el grado de **Licenciatura en Ingeniería en Tecnologías de Información**, de las personas estudiantes, **Michelle Rodríguez Hernández,** cédula de identidad, **604550898; William García Molina,** cédula de identidad, **604360917**.

Reunido el Tribunal Evaluador, los aspirantes procedieron a presentar y defender su Proyecto de Graduación titulado, **"Analizar los controles para la seguridad, de la información implementados, por la empresa distribuidora COARSA, en San Ramón de Alajuela, de acuerdo con la norma ISO- 27002, durante el segundo semestre del año 2022".**

Concluida la presentación y defensa del Proyecto de Graduación, el Tribunal Evaluador consideró que, de conformidad con la normativa en la materia, las personas estudiantes obtuvieron una calificación de 99, cumpliendo con las exigencias requeridas para la aprobación del Proyecto y les es conferido el grado de **Licenciados en Ingeniería en Tecnologías de Información.**

No ( ) Si (x) mención honorífica

Oberto Santín Cuesta
Profesor Tutor

Roberto Escobar Agüero
Lector

Erick Saborío Berger
Representante del Sector Productivo

Antonieta González Esquivel
Presidente del Tribunal Examinador

Sello

Universidad Técnica Nacional
Tecnologías de Información

Estudiantes:

William García M.

Michelle Rodríguez Hernández
Cédula, 604550898

William García Molina
Cédula, 604360917

Tabla de contenidos

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

GLOSARIO DE ABREVIATURAS

COARSA: Distribución y cobertura de calidad.

ISO: Organización Internacional de Normalización.

Agradecimientos y dedicatoria

William

Agradecimientos

Quiero expresar mi más sincero agradecimiento a mi familia por su constante amor y apoyo. También quiero reconocer a mis profesores, Oberto Santín Cuesta y Floribeth Vindas Parra, ambos docentes espectaculares, cuya guía invaluable no solo en las aulas, sino a lo largo de todo el proyecto, ha sido fundamental para este logro. Además, mi gratitud se extiende a todas las personas que de diversas formas me brindaron su apoyo a lo largo de esta travesía. Reconozco que son muchos para nombrar, pero les agradezco de corazón.

Dedicatoria

Dedico este logro a Dios, quien me ha proporcionado la fortaleza y la sabiduría para persistir a pesar de los desafíos. A mi abuela, Yuvani Alvarado Ocampo, una gran mujer que siempre fue mi constante apoyo y que me inspiró a dar lo mejor de mí. A mi hermano, Justin García, por su inquebrantable presencia a mi lado. A mis padres y a toda mi familia, quienes me han respaldado de innumerables maneras. Mi profundo cariño y agradecimiento van hacia todos ustedes.

Michelle

Agradecimientos

En primera instancia, agradezco a mis padres, que desde el inicio me han brindado todo el apoyo, y herramientas para poder cumplir cada uno de los objetivos personales y académicos, por motivarme a seguir adelante, sin importar los obstáculos que hallan en el camino. El cariño, y esfuerzo que mis padres han tenido que realizar para poder salir adelante, y estar donde estoy en este momento, es algo que es de admirar.

Así mismo, estoy sumamente agradecida con aquellas personas que fueron de gran importancia en este proceso, que de una u otra forma, me dieron ese impulso para seguir adelante, para continuar con mis estudios, y ser ese gran apoyo, de muchas maneras diferentes, en momentos de dificultad.

Y no sin antes, le agradezco al equipo de trabajo detrás de este gran proyecto, a mi tutor por brindarnos esa guía desde el inicio de este proceso. A los lectores por la dedicación, y a los profesores que, con su dedicación y paciencia, transmitieron sus conocimientos para ser una excelente profesional.

Dedicatoria

Agradezco a cada una de las personas que fueron parte esencial de mi camino académico y personal. A mis padres, que tienen derecho a un merecido reconocimiento, por luchar y dar todo de sí, por cada sacrificio y apoyo, para que lograrán concretar con éxitos los estudios; creciera como una gran profesional, y motivarme a seguir adelante; es un orgullo y privilegio ser su hija.

A todos aquellos, que de alguna u otra forma, fueron parte de este gran proceso, al ser de impulso en mis momentos más difíciles, y no sin antes, agradecerle a esa persona que, con el paso del tiempo, se convirtió en parte importante de esta historia, y apoyarme en cada etapa.

Resumen

En los últimos años, la ciberseguridad se ha convertido en un elemento imprescindible para las organizaciones y la empresa Distribuidora COARSA no es la excepción, por esta razón se decidió realizar el proyecto Analizar los Controles para la Seguridad de la Información Implementados por la Empresa Distribuidora COARSA, en San Ramón de Alajuela, de acuerdo con la Norma ISO 27002, durante el Segundo Semestre del año 2022.

Esta iniciativa tuvo como finalidad primordial enriquecer las prácticas de ciberseguridad en la organización, priorizando en particular el fortalecimiento de los controles de índole física y tecnológica. El objetivo primordial consistió en prevenir el acceso no autorizado a la información sensible, además de situar a la empresa en la vanguardia de la seguridad a través de políticas progresistas.

Los logros obtenidos en el curso de este proyecto fueron sumamente alentadores. Destaca, en particular, la concepción de dos sólidas Políticas de Seguridad: una dedicada a los Controles Físicos y otra enfocada en los Controles Tecnológicos. Ambas políticas, elaboradas con base a los parámetros delineados en la Norma ISO 27002:2022.

Simultáneamente, la ejecución de un análisis exhaustivo proporcionó al equipo de Tecnologías de la Información una visión detallada de las fortalezas y vulnerabilidades inherentes a la empresa. Permitiéndoles identificar las áreas más susceptibles a riesgos potenciales.

Introducción

La presente investigación consiste en un análisis de los controles físicos y tecnológicos implementados por la empresa Distribuidora COARSA, para la seguridad de la información, basándose en lo establecido según la Norma ISO 27002:2022, cabe destacar que la empresa se encuentra ubicada en el cantón de San Ramón, perteneciente a la provincia de Alajuela. El proyecto se enfocó en reconocer cómo la organización implementa los controles físicos y tecnológicos para la protección de la información; asimismo, dichos controles se contrastan con lo indicado por la Norma en sus capítulos VII y VIII, para finalmente desarrollar una política de seguridad.

Por otra parte, la principal razón por la cual se realizó esta investigación se debe los recientes acontecimientos, a nivel nacional e internacional, como el robo de información, *hackeos* y explotación de vulnerabilidades en sistemas que manejan datos sensibles, por motivos como este, son necesarias las investigaciones como la presente, que busca el desarrollo e implementación de políticas y normas que les permitan a las organizaciones actuar de manera correcta ante amenazas que comprometan la seguridad de la información.

Por otro lado, cabe mencionar que la investigación se realizó bajo el enfoque mixto, porque permitió recopilar, analizar e integrar la información tanto de manera cualitativa como cuantitativa, abordándolos de diferentes puntos de vista y enriqueciendo los resultados obtenidos. Se optó por este enfoque, por la versatilidad que brinda, debido a que utiliza ventajas de ambos, cuantitativos y cualitativos, los cuales permitieron generar resultados más detallados y con una alta fiabilidad.

Además, la metodología empleada hizo uso de varios tipos de investigación, que permitieron cumplir con los objetivos planteados, entre ellos destacan la investigación de campo, utilizada por la necesidad de realizar una serie de visitas que permitieran recopilar la información necesaria para determinar cómo se implementa el control físico y tecnológico en la empresa; se usó también, la investigación documental, porque permite la revisión de documentos, manuales y normas, para determinar lo establecido en la Norma ISO 27002, con respecto a los controles físicos y tecnológicos para la gestión de la seguridad de la información.

Así mismo, se utilizó la investigación aplicada, al contrastar lo establecido en la Norma ISO 27002 con respecto al control físico y tecnológico, y las prácticas de control implementadas en la empresa, se optó por esta porque ayudó a generar un enlace entre la teoría y el producto, en este caso, la política de seguridad de controles físicos y tecnológicos, como resultado de esta investigación.

Por otro lado, la población consistió en 104 funcionarios de distintos departamentos de la empresa Distribuidora COARSA, los cuales tenían aproximadamente cinco años de laborar para esta compañía al momento de la investigación. La muestra fue de 51 funcionarios de diferentes áreas de la organización, incluyendo el Departamento de Tecnologías de Información, dicha muestra se utilizó en vista de que era necesario involucrar a todo el personal que estuviera relacionado de algún modo con la seguridad de la información, otro motivo fue la necesidad de optimizar el proceso de recolección y tabulación de los datos.

Por otra parte, las técnicas e instrumentos manejados en la investigación se relacionaron con la observación, la cual se usó para corroborar que se cumplieran

los controles físicos y tecnológicos, permitiendo identificar cuáles no se estaban cumpliendo. También se utilizó la encuesta, construida con base en lo indicado en la Norma ISO 27002, con respecto a los controles físicos y tecnológicos, constó de una serie de preguntas relacionadas, que se aplicaron a la totalidad del personal de Tecnologías de Información y a una parte de los funcionaros de los demás departamentos.

Por otro lado, otra técnica de gran utilidad fue la revisión bibliografía, porque permitió hacer uso de artículos, revistas, páginas web oficiales y manuales que facilitaron determinar lo establecido en la Norma ISO 27002, con respecto a los controles físicos y tecnológicos para la gestión de la seguridad de la información. Además, se desarrollaron dos listas de cotejo, una con base en los controles físicos y otra en los tecnológicos, las cuales permitieron contrastar lo establecido en la Norma ISO 27002 con respecto al control físico y tecnológico, y las prácticas de control implementadas en la empresa Distribuidora COARSA.

Por otra parte, una vez aplicados los instrumentos, se procedió a realizar un proceso de análisis y tabulación de los datos mediante tablas, gráficos y cuadros, utilizando los datos obtenidos tras la recopilación, el cual permitió interpretar los resultados y desarrollar una política de seguridad para la empresa, de acuerdo con la Norma ISO 27002:2022, que les permitiera atender los aspectos no documentados, relacionados con el control físico y tecnológico de la organización.

Una de las conclusiones a las que se llegó una vez finalizado el trabajo, es la importancia de controles que permitan minimizar los efectos de cualquier incidente que se pueda presentar y que afecten la información de la empresa.

Capítulo I

Introducción

Objetivos

1.1 Tema

Analizar los controles para la seguridad de la información, implementados por la empresa Distribuidora COARSA, en San Ramón de Alajuela, de acuerdo con la Norma ISO 27002, durante el segundo semestre del año 2022.

1.2 Área de estudio

El área de estudio de esta investigación es la tecnológica, enfatizando en la seguridad de la información, específicamente en los controles físicos y tecnológicos de los equipos informáticos, haciendo uso de los capítulos VII y VIII de la Norma ISO 27002:2022, que rigen aspectos como el establecimiento de directrices y principios generales que permiten implementar, mejorar y mantener la gestión de la seguridad de la información en una empresa.

1.3 Justificación

La presente investigación se enfocará en identificar y contrastar los controles para la seguridad de la información, implementados por la empresa Distribuidora COARSA, en San Ramón de Alajuela, de acuerdo con la Norma ISO 27002:2022, lo anterior, debido a la importancia que tiene la tecnología y los sistemas de información para las empresas, dado que estas se han convertido en elementos indispensables, en vista de que son cada vez más los datos que se debe manejar, siendo su mayoría muy sensibles. Además, con su ayuda se logra optimizar y mejorar los procesos relacionados con la producción, ventas, cobros e incluso, las

capacitaciones. Lo anterior provoca que las organizaciones deban estar a la vanguardia cuando se trata de tecnología y aún más, si son sistemas de información. Algunos autores afirman que la información es el alma de las empresas, Linares (2022) indica lo siguiente:

> Los datos, de la mano de la cultura de la innovación, se han convertido en grandes aliados de las compañías para crecer. No solo permiten conocer mejor al mercado, proteger la privacidad, sino también alcanzar a potenciales clientes, acercarse al personal y guiar a las empresas en lo que necesitan para potenciar su negocio. (párr. 1)

Lo anterior permite ver más allá de los típicos procesos que se realizan en toda organización, tomando en cuenta temas como la innovación y cómo los datos se han convertido en los aliados de las empresas, debido a que brindan una serie de beneficios que contribuyen a su crecimiento. Por esta razón, la información es de suma importancia para las compañías, más que todo en una era cuando lo digital cada vez toma más fuerza y la competencia crece exponencialmente. Al respecto Terreros (2021) afirma lo siguiente:

> Actualmente hay una relación directa entre los resultados exitosos de una compañía y el uso de sistemas de información. Sin embargo, no se trata de que un negocio se llene de sistemas y software, sino de que haya un análisis de las necesidades de la empresa y de la operación que tiene, y decidir una

> implementación estratégica de estas plataformas para que realmente contribuyan a cumplir los objetivos de una empresa. (párr.7)

Las afirmaciones de la autora hacen ver que no solamente se trata de implementar sistemas de información, sino que además, es importante realizar análisis que permitan que la empresa cumpla sus objetivos de la mejor manera y para eso, una parte muy importante es la seguridad física y tecnológica.

De acuerdo con lo anterior, es común que las organizaciones busquen formas de hacer un análisis físico y tecnológico de sus activos, basándose en normas internacionales o buenas prácticas; existe una serie de organizaciones y bibliotecas, como la Organización Internacional de Normalización (ISO) y la Biblioteca de Infraestructura de Tecnologías de Información (ITIL), que se encargan de crear normativas y buenas prácticas que permiten mejorar la calidad de los sistemas de gestión en las empresas, garantizar la eficiencia y, además, ayudan a los encargados del Departamento de Tecnologías de Información a llevar un control tanto físico como tecnológico. “Es importante que la empresa u organización establezcan requisitos de seguridad principales para poder evaluar las amenazas, realizando una estrategia en conjunto con los objetivos de la empresa para así estimar la probabilidad de que estos se produzcan” (Guerrero, 2021, p. 7). Igualmente, la seguridad se ha convertido en un tema de suma importancia para cualquier entidad, el uso de normas para la gestión de la información se ha vuelto indispensable, principalmente por el aumento de ciberataques que se ha visto en los últimos meses, López (2022) afirma que:

> Los ciberataques a los gobiernos se están volviendo cada vez más comunes y América Latina ya ha sufrido varios ataques en los últimos meses. Aunque tradicionalmente (…) han apuntado a objetivos en América del Norte y Europa, el interés en otras regiones está creciendo. (párr.6)

Ataques como los que menciona el autor, se han presentado en los últimos meses en el país, empresas del sector público como la Caja Costarricense del Seguro Social y el Ministerio de Hacienda han sido blancos fáciles para los ciberdelincuentes que operan desde el extranjero, por esta razón, es necesario el desarrollo e implementación de políticas y normas de seguridad que permitan evitar este tipo de eventos.

Por otra parte, es fundamental que los profesionales empleen distintos métodos de recopilación de información para analizar detalladamente la situación y las necesidades de la empresa, a fin de garantizar que las políticas de seguridad que se implementen sean adecuadas para los requerimientos específicos. En el caso de la Distribuidora COARSA, los dueños y responsables del Departamento de Tecnologías de la Información decidieron centrarse únicamente en los capítulos VII y VIII de la Norma ISO 27002:2022, debido a que se enfocan en la protección de la parte física, como las instalaciones y oficinas donde se maneja información sensible, y en la infraestructura tecnológica que puede verse gravemente afectada por un posible ciberataque o una violación de la seguridad de la organización. No obstante, esto no significa que se descuide la seguridad de la información de manera general, sino que, se prioriza la protección de los aspectos más críticos en el momento en el

que se realiza la presente investigación. Cabe destacar que una estrategia de seguridad de la información más amplia implicaría un mayor consumo de tiempo y recursos que en este momento no son viables para la empresa en cuestión.

Con base en lo anterior, este proyecto de investigación es relevante, porque permite determinar la situación actual de la empresa Distribuidora COARSA, con el fin de analizar el control físico y tecnológico para la gestión de la seguridad de la información, además de desarrollar una política que le ayude a la organización a estar a la vanguardia en cuanto a normas de seguridad y controles tanto físicos como tecnológicos.

1.4 Estado del arte

El estado del arte es la comprensión del estado del conocimiento sobre un objeto de estudio, en determinado momento; en tal sentido, se ordena, integra y analiza periódicamente el conjunto de informaciones, desde diferentes perspectivas (Mendívil, Sánchez, Cabrera y Bustamante, 2021).

Teodoro Kelvin Salazar, realiza en el año 2018 su proyecto de investigación denominado “Análisis de la norma ISO/IEC 27002:2013 para mejorar los controles de la seguridad de la información en la Sala de Cómputo #14 de la carrera de Ingeniería en Computación y Redes”.

Los métodos utilizados para llevar a cabo la investigación, fue el hipotético-deductivo, que facilitó el planteamiento adecuado de la investigación, además del

método exploratorio para ejecutar la propuesta planteada acorde con las políticas de la Norma ISO 27002:20013.

Como herramientas de recolección de datos, Salazar realizó encuestas, entrevistas y observación directa como técnicas para la recaudación de los datos.

La población utilizada para la recolección de datos consiste en los estudiantes, docentes y el técnico de la sala de cómputo #14 de la carrera de Ingeniería en Computación y Redes, para un total de 196 participantes, con una muestra de 125, obtenida por medio de una fórmula matemática.

Al finalizar la investigación, el autor halla que la Institución no cuenta con políticas ni medidas de seguridad implementas, lo que hacía que la Universidad se hallase vulnerable ante distintas amenazas, por lo tanto, elaboró un manual técnico para que sea utilizado como medida de seguridad por los alumnos e implementó el software GpG4Win-Kleopatra, con el fin de proteger los datos almacenados en los equipos de cómputo.

Ledy Ruth Sandoval Fernández, en el año 2019, para optar por el título profesional de ingeniera en Sistemas y Computación, desarrolló su proyecto “Modelo de buenas prácticas aplicando ISO 27002 para la gestión de incidencias de la red Wncor”.

Por medio de cuestionarios que la autora le realizó a una población 500 usuarios, con una muestra de 39.33, usuarios pertenecientes al grupo *IASUSER* en el *active directory* y que contaban con acceso a la red Wncor, para la conocer desde

el punto de vista del consumidor sobre los incidentes que han tenido con la red Wncor.

Para el desarrollo de su proyecto utilizó la investigación aplicada que le facilitó la aplicación de las buenas prácticas que brinda la Norma ISO 27002, para la gestión de las incidencias que se reportaban a diario. Por otro lado, con ayuda de la investigación preexperimental que le permitió tener un mayor control de las variables que se encontraron durante la investigación y así obtener resultados más precisos.

Al finalizar la investigación, Sandoval realizó una prueba en la red Wncor, durante cuatro semanas, implementando los controles de la Norma ISO 27002, de roles de acceso y gestión de activos, obteniendo buenos resultados; los problemas de conexión a la red e ingreso a los *file servers* se vieron reducidos.

Dalton Gonzalo Hernández García, en el año 2019, para optar por el grado de Magister en Seguridad Informática Aplicada, desarrolló su proyecto “Diseño e implementación de un esquema de seguridad de nivel 0 a nivel 1 basado en las normas ISO 27002:2013”.

Hernández hace uso de técnicas de recolección de datos con base en la observación en la empresa, permitiéndole realizar un análisis cualitativo para conocer datos, como el nivel competitivo y el cumplimiento de normativas. Asimismo, realizó un análisis cuantitativo para evaluar el impacto a nivel monetario, en caso de ocurrir algún incidente en el proceso industrial o en un activo.

En el desarrollo de la investigación se enfrentó la dificultad sobre cómo se iba a desarrollar e implementar el nivel de seguridad para que estuviesen alineados con los objetivos planteados al inicio de la investigación y a las necesidades de la empresa. Es importante tener presente que la Institución no contaba con ningún control o política de seguridad, por lo tanto, la protección de los datos era nula y no existía plan de recuperación.

Se aplicó una identificación de los activos que la empresa poseía, para determinar los riesgos que se encontraban relacionados con la infraestructura tecnológica, igualmente, se debió establecer las posibles dimensiones sobre las cuales se realizaría la valoración, para conocer el valor de los activos, identificar las amenazas y vulnerabilidades, estimar daños futuros y, por último, clasificar los riegos que se reconocieron.

José Miguel Fuentes Caro realizó en el año 2019 su proyecto final de graduación, titulado “Auditoría al sistema de gestión de seguridad de la información del proceso de gestión de incidentes de ANS Comunicaciones, con base en la norma técnica colombiana NTC-ISO/IEC 27002”, con el fin de especializarse en el área de Auditoría de Sistemas de Información.

Para realizar este estudio y Con base en la propuesta planteada al inicio de la investigación, se hizo una serie de entrevistas al personal con diferentes grados de responsabilidad, dentro del proceso de incidentes de cliente de *networking*, de ANS Comunicaciones, vía Meet de Google y correo electrónico. Además de

entrevistar a la gerente de operaciones, al supervisor y operador de gestión de incidentes, que fueron puntos importantes para lograr el cumplimiento de los objetivos planteados.

Por otra parte, se desarrolló una auditoría dentro de la empresa para tener una mejor idea de la situación de la industria en ese entonces, en la cual se ejecutó un total de seis pruebas guiadas durante dos días. Con base en los resultados que arrojaron las pruebas, se hallaron disconformidades en el control de acceso a redes, manejo de información secreta, acceso a la aplicación OSTicket y en las políticas de divulgación de información.

En el informe que se realizó con base en las pruebas de auditoría y los descubrimientos hallados, se recomendaron directrices y acciones para implementar al sistema general de seguridad de la información del proceso de gestión de incidentes de clientes de *networking* de ANS Comunicaciones.

Jorge Luis Figueroa Leyton desarrolla su proyecto de investigación “Plan de seguridad informática basado en la Norma ISO 27002 y la gestión de la información para el Departamento de TIC de la Uniandes Extensión Babahoyo”, para la obtención del grado de Licenciatura en el año 2019.

La infraestructura tecnológica encargada del cumplimiento de las demandas de las distintas unidades que tiene la Institución carecía de sistema de monitoreo de controles, acceso de control en los laboratorios de cómputo, seguridad,

inventario, y faltas de informes de la infraestructura de red, lo que motivó al autor a realizar la investigación.

El autor hizo uso de una investigación de tipo bibliográfica para fundamentar el plan de seguridad informática y la gestión de la información y con trabajo de campo, que fue de ayuda para la recopilación de datos por medio de encuestas y entrevistas realizadas a una población de 25 trabajadores, en las cuales se incluyeron a 20 administrativos y cinco directivos de la empresa; no hizo uso de muestra debido al tamaño de la población.

Al concluir su investigación, hizo entrega de una propuesta que incluía el análisis de riesgo en conjunto con su evaluación, conformada por la identificación de activos, requerimientos legales y comerciales, amenazas, vulnerabilidades y probabilidad de incurrencia y valoración de los activos. También hizo entrega del tratamiento de riesgo y de la toma de decisiones a nivel gerencial, el riesgo residual, y selección de los controles que se recomienda implementar.

En el año 2020, Miguel Ángel Colmenares Rodríguez realizó su proyecto final de graduación titulado “Auditoría al control de acceso del sistema de información Proyecto INNpulsa-udea de la Interventoría de la Universidad de Antioquía bajo la norma ISO/IEC 27002”, para especializarse en auditoría de sistemas de información.

El autor desarrolló su trabajo mediante la línea de investigación de Software Inteligente y Convergencia Tecnológica para la identificación de conceptos de

auditoría de aplicaciones, siendo necesarios para un adecuado uso del ISO/IEC 27002, así como el control de acceso del sistema de información. Hizo uso de aspectos metodológicos de COBIT, COSO y la ISO, con el objetivo de la evaluación de buenas prácticas en las políticas de control de acceso.

Este proyecto se enfocó en la observación como técnica de recolección de datos, en la que realizó cuestionarios a funcionarios de la Universidad e Antioquía y del INNpulsa Colombia.

Los cuestionarios se aplicaron para el reconocimiento del control de acceso del aplicativo y una evaluación del sistema de control interno, definiendo riesgos y controles para luego realizar el diseño y la ejecución de pruebas.

Durante la evaluación de los controles de acceso, el autor propuso una auditoría, con base en la Norma ISO 27002, enfocada en los controles definidos y aplicables en el dominio Control de Acceso que permita hacer entrega de un informe general de este.

Al finalizar con las distintas pruebas que se realizaron en la empresa para estimar el control de acceso del Sistema de Información de la Interventoría, se logró demostrar que la mayoría de los lineamientos que se establecen en la ISO/IEC 27002, se cumplen, lo que aporta un valor significativo a la seguridad.

Manuel Alfredo Sánchez Vela, para optar por el grado de Licenciatura, realizó su proyecto final de graduación titulado “Elaboración de un plan de seguridad informática para mejorar la gestión de la información de la subgerencia de

tecnología de la información, de la Municipalidad Provincial de Requena–2021”, en el año 2021.

Por medio de una encuesta realizada al personal de la Municipalidad, recopiló los datos necesarios para conocer de primera mano la seguridad informática del ayuntamiento, con respecto a la gestión de la seguridad y con una muestra de 13 personas.

Por otra parte, por medio de procedimientos y análisis de datos, recopilados por instrumentos como cuestionarios y ficha de observación, desarrolló un plan de seguridad adecuado a las necesidades que la Municipalidad tenía en ese momento.

Lo anterior le permitió una evaluación real sobre la protección de los datos, determinando que el peligro existente en ese momento era alto, estando en riesgo los archivos de los equipos de cómputo.

Otros hallazgos significativos correspondieron a que los equipos no recibían mantenimiento por parte de la Municipalidad, la base de datos y los sistemas de seguridad, además, no tenían establecidos ningún control de seguridad tanto en la instalación como de funcionamiento.

En el año 2021, Diana Carolina Murillo Pin realizó el proyecto “Políticas de seguridad de la información basado en Normas ISO 27002 para el Departamento Informático de la Universidad Estatal del Sur de Manabí”, para optar por el grado de Licenciatura.

La investigación se realizó mediante el método exploratorio, lo que le facilitó determinar las políticas correctas de la Norma ISO 27002, para fortalecer la seguridad del Departamento, además del uso de técnicas de observación, que le permitieron realizar un análisis de la información de forma interpretativa y crítica, para determinar el nivel de riesgo que existía debido a la falta de políticas de seguridad.

Como parte del análisis de la información, se le realizó una entrevista al jefe del Departamento de Sistemas Informático de la Universidad, para conocer si la Institución contaba con aspectos organizativos para la seguridad, políticas de seguridad, gestión de activos, controles de acceso a la Institución, plan de continuidad, licencias de los programas utilizados y mantenimiento de los sistemas informáticos; en este caso, al ser solo una persona como parte de la población, no fue necesario realizar el cálculo de la muestra.

A lo largo del documento, Murillo explica ampliamente las amenazas y sus diferentes variantes, así como los distintos ciberdelincuentes, para tener una mayor comprensión del porqué suelen atacar a la red de las distintas organizaciones a nivel global. El uso de instrumentos con los que suelen violentar la infraestructura informática, y los riesgos y vulnerabilidades a los que se encuentra expuesta la Universidad.

La autora hace inclusión de herramientas básicas que se puede implementar para prevenir ataques informáticos, como una infección. Menciona algunos

programas y acciones que permiten certificar la seguridad del dispositivo, como el uso de un navegador y sistema operativo actualizado, no abrir archivos enviados por remitentes desconocidos, entre otras tácticas importantes.

1.5 Objetivos

1.5.1 Objetivo General

Analizar el control físico y tecnológico para la gestión de la seguridad de la información de la empresa Distribuidora COARSA, en San Ramón de Alajuela, de acuerdo con la Norma ISO 27002, durante el segundo semestre del año 2022.

1.5.2 Objetivos Específicos

- Identificar cómo se implementa el control físico y tecnológico en la empresa Distribuidora COARSA, mediante diferentes técnicas de recolección de datos.
- Determinar lo establecido en la Norma ISO 27002, con respecto a los controles físicos y tecnológicos para la gestión de la seguridad de la información, mediante revisión documental.
- Contrastar lo establecido por la Norma ISO 27002 con respecto al control físico y tecnológico, y las prácticas de control implementadas en la empresa Distribuidora COARSA, por medio de técnicas de análisis de datos.
- Desarrollar una política de seguridad para la empresa COARSA, de acuerdo con la Norma ISO 27002, que les permita atender los aspectos no documentados, relacionados con el control físico y tecnológico en su organización.

Capítulo II

Marco Teórico

Marco teórico

Se presenta en el siguiente apartado, una comprobación de los aspectos teóricos más relevantes y de la investigación.

2.1 Seguridad de la información

Mauricio Diéguez (2022) indica que:

> Es una guía de implementación de buenas prácticas de seguridad, desde una perspectiva holística e integrada, que busca disminuir las vulnerabilidades de la organización a través de la implementación de un sistema de gestión de la seguridad de la información. (p. 14)

La información se ha vuelto un objeto intangible de mucho valor, por lo tanto, la protección debe de ser de forma precisa, con ayuda de estrategias adecuadas, para prevenir el uso no autorizado y detectar a tiempo las amenazas.

María (2019) en su investigación aporta que:

> La información representa uno de los activos de mayor valor que posee toda empresa y es trascendental ya que se utiliza tanto en las tareas diarias como en la toma de decisiones estratégicas. Cualquier pérdida, daño o alteración de esta podría provocar serios problemas para el funcionamiento normal de las operaciones y hasta podría significar graves pérdidas económicas. (p. 19)

Marcos Espinoza (2019) considera que la seguridad de la información:

> Es un asunto corporativo y es por esta razón que la perspectiva correcta para llegar a un cumplimiento regulatorio satisfactorio es tratando a esta actividad desde un enfoque de gobierno, el cual es transversal en toda la organización no solamente un enfoque hacia los sistemas de información. (p. 1)

Es recomendable integrar a la empresa a un gerente de seguridad de la información que incorpore los conocimientos necesarios para mejorar la estrategia de seguridad de la información por medio de acciones y elementos necesarios, que en conjunto dé con la parte más básica y esencial de la organización, como los trabajadores; son componentes fundamentales para garantizar la protección de los datos.

2.2 Políticas

Corvo (2021) lo define como “la estrategia con respecto a los principales puntos considerados en el área de tecnología de información, con el fin de proponer acciones y medidas para asegurar la protección de los medios de información y los datos” (párr. 1).

En informática se trata de estándares que se aplican basados en las necesidades de la organización que cada cierto tiempo se actualizan o modifican, según los requerimientos que la empresa tenga en ese momento, siendo su objetivo principal la gestión adecuada de la confidencialidad, integridad y disponibilidad de

la información, tomando en cuenta cómo los trabajadores e interesados se relacionan con los activos.

2.3 Políticas de seguridad

El artículo escrito por Vázquez Domínguez (2019) indica que por política informática se entiende “al conjunto de planes, programas y acciones en el ámbito de tecnologías para el tratamiento de la información, la protección y la seguridad de los datos y medios informáticos” (p.4).

Antes de realizar políticas de seguridad para una empresa, se debe de tener claras las necesidades que la organización posee, en cuanto a seguridad física como lógica, por medio de inventarios, documentación, para posteriormente, hacer un estudio de los riesgos posibles y actuales, así como la identificación de las distintas amenazas. Una vez realizado el estudio pertinente, se implementan las políticas de seguridad basadas en las necesidades.

Cesar Vega (2018) indica que antes de implementar las políticas de seguridad en una empresa, es importante tomar en cuenta la tecnología que la empresa posee, por lo que, en su artículo, de forma más amplia explica que:

> Primero que se debe tener en cuenta es hacer un análisis observatorio de todas las posibles amenazas que podrían suscitarse considerando la tecnología que posee la institución, con esta estimación de pérdidas se podrían analizar las preguntas, escenario y controles a ser considerados para su implementación. (p. 10)

Por lo que la Norma ISO/IEC 27001 añade que “se debería definir un conjunto de políticas para la seguridad de la información, aprobado por la dirección, publicado y comunicado a los empleados, así como a todas las partes externas relevantes”.

Por lo tanto, al momento de implementar las políticas, es importante que se encuentren acorde con las decisiones tomadas con respecto a la seguridad, en las cuales todos los miembros de la empresa se encuentren presentes, para que se tome la mejor decisión.

2.4 Norma

IRAM (2022) sostiene que “son documentos que surgen del trabajo de un grupo de expertos que acuerdan las condiciones mínimas que debe tener un producto, servicio o sistema de gestión” (párr. 1).

Alonso (2022) lo define como “un conjunto de estándares con reconocimiento internacional que fueron creados con el objetivo de ayudar a las empresas a establecer unos niveles de homogeneidad en relación con la gestión, prestación de servicios y desarrollo de productos en la industria” (párr. 1).

Las normas se van creando conforme a las necesidades que existan en ese momento o para prevenir incidentes y regular comportamientos, que como lo indican los autores, suelen tratarse de documentos establecidos o creados por algún organismo para que las empresas cumplan con estándares de calidad, tanto en los servicios/productos que se ofrecen, como en la gestión.

Sofía Riesco (2018) dice que “es un documento de aplicación voluntaria por parte de una empresa que contiene especificaciones técnicas basadas en los resultados de la experiencia y el desarrollo tecnológico” (párr. 1).

Cabe recalcar que las normas no son de aplicación obligatoria, pero se le recomienda a la empresa aplicar las directrices que se considere adecuadas basadas en lo que se busca alcanzar.

2.5 Tipo de normas de seguridad

La seguridad de la información no abarca solamente un área, sino que, su objetivo es proteger la infraestructura tecnológica y todo lo que lo compone, desde el hardware al software, así como la manipulación por parte del usuario final, que en muchas ocasiones, suele ser el causante de incidentes y alteraciones a la protección de los activos.

Es importante mencionar que pertenecen a la familia de la ISO/IEC 27000 y son estándares de confiabilidad que se encuentran supervisados por el área de ITIL e implementadas para las buenas prácticas dentro de la industria.

Seguidamente se presentan las distintas Normas ISO 2700, familia de las normas de seguridad.

1. ISO 27001, está conformada por los requisitos de la SGSI, además de tratarse de la norma principal normal, ante todo, porque los auditores externos se encuentran certificados.

2. 27004, especifica recomendaciones para gestionar la seguridad y quién, cuándo y cómo medirlos.

3. 27005, gestión y evaluación de riesgos de seguridad, y una entidad externa debe de implementarlas mediante dos auditorías detalladas.

Cabe recalcar que, de los controles que cada ISO contiene, sólo se escoge implementar los que se consideren esenciales para el cumplimiento del objetivo dentro de la organización.

2.6 Norma ISO

Sonia López (2019) indica que:

> Son las siglas en inglés International *Organization for Standardization*. Se trata de la Organización Internacional de Normalización o Estandarización, y se dedica a la creación de normas o estándares para asegurar la calidad, seguridad y eficiencia de productos y servicios. (párr.1)

César Alonso (2022) lo define como:

> Las normas ISO son un conjunto de estándares con reconocimiento internacional que fueron creados con el objetivo de ayudar a las empresas a establecer unos niveles de homogeneidad en relación con la gestión, prestación de servicios y desarrollo de productos en la industria. (párr.1)

Como se señala anteriormente, se trata de una organización a nivel global, que crea diversas normativas tanto nacionales como internacionales, con el propósito de brindarles a las empresas una guía para que establezcan y garanticen el buen funcionamiento, así como la mejora de la gestión, obteniendo un mayor desempeño, posicionándolo en el mercado laboral al ofrecer productos/servicios de calidad.

2.7 Características de la ISO

Se fundó el 23 de febrero de 1947 en Suiza, Ginebra, siendo una entidad no gubernamental, hallándose en más de 200 países en la actualidad, cuya finalidad es la creación de estándares internacionales para promover el uso de estándares privativos, industriales y comerciales. Se establecieron siete normas, que se subdividen según los intereses, necesidades y objetivos de la empresa:

1. ISO 13485: Dispositivos médicos.
2. ISO 9000: Gestión de calidad.
3. ISO/IEC 17025: Laboratorio de prueba y calibración.
4. ISO/IEC 27000: Gestión de seguridad de sistemas informáticos.
5. ISO 1400: Gestión ambiental.
6. ISO 26000: Responsabilidad social.
7. ISO 13485: Productos sanitarios.

2.8 ISO 27002

Evans (2022) indica que la norma “ISO 27002 profundiza en los detalles sobre cómo se pueden implementar los controles” (párr. 4). Si bien, para obtener una certificación de seguridad deben de acudir a la Norma ISO 27001, la ISO 27002 es utilizada como reseña para la aplicación de los controles. Según la ISO 27002, los activos pueden clasificarse como:

1. Recursos de la información, como la documentación, manuales de usuario y procedimientos, entre otros.
2. Recursos de software, aplicación y SO, entre otros
3. Activos físicos, mobiliarios, dispositivos físicos.
4. Servicios.

Es de importancia que se realice una identificación de activos en la empresa, para calcular el valor que tiene, conocer los roles que existen dentro de la organización y las características, para proceder con una clasificación, basándose en la sensibilidad y el riesgo de la información contenida.

Lo anterior se puede realizar con ayuda de herramientas como una matriz de riesgos, con el fin de elegir las políticas adecuadas para la protección de la información. Se destaca, porque se implementa por seis aspectos que le facilitan al auditor el estudio e implementación con base en lo que la empresa necesite.

1. Plan de seguridad de riesgos.
2. Política de seguridad detallada.

3. Departamento de gestión de activos.
4. Administración de operación y puntos de acceso.
5. Departamento de sistemas y mantenimiento de información.
6. Sistemas de control de incidentes.

2.9 ISO 27002:2022

El 15 de febrero se publica la versión 2022, siendo una mejora a la versión de 2013, aunque se debe tomar en cuenta que después de cinco años de haber sido publicada la ISO, se realiza una evaluación para ver si se necesita una renovación o debe de eliminarse.

Algunos de los controles de la 27002:2013 se unieron a la nueva versión, con el fin de obtener estándares más actualizados a las necesidades presentes de las empresas. Cabe recalcar que del documento sólo se encuentran las versiones en inglés y holandés.

Entre las mejoras encontradas en esta ISO, destaca que, en comparación con la versión de 2013, existe una reducción de los controles, que pasó de ser de 114, distribuidos en 14 dominios, a cuatro dominios, con un total de 14 controles.

2.10 Características de la ISO/IEC 27002:2022

Esta versión se nombró como “Controles de Seguridad de la Información”, con la incorporación de 11 nuevos controles y 16 términos que permiten un alcance más amplio de la ciberseguridad. Además de que se le añaden nuevos términos y definiciones para facilitarle el entendimiento al usuario. La estructura se ve

modificada, para asegurar una mayor seguridad de la información, incluidos los atributos de los controles se ven afectados. Cuenta con cuatro grupos de cláusulas, conformados por:

1. Controles organizacionales (37).
2. Controles de personas (8).
3. Controles físicos (14).
4. Controles tecnológicos (34).

2.11 Tipos de atributos de la ISO 27002:2022

La Norma los señaló con el símbolo conocido como *hashtag* (#), para hacer de la búsqueda del término más fácil.

a) Tipo de control:

#Preventivo, busca evitar que ocurra un incidente.

#Detectivo, actúa en el momento en que ocurre el incidente.

#Correctivo, actúa cuando el incidente ocurrió para corregir la acción y así disminuir la posibilidad de uno nuevo o eliminarlo.

b) Propiedades de seguridad de la información:

#Confidencialidad.

#Integridad.

#Disponibilidad.

c) Conceptos de ciberseguridad (tomados de la ISO/IEC TS 27110):

#Identificar.

#Proteger.

#Detectar.

#Responder.

#Recuperar.

d) Capacidades operativas:

#Gobierno.

#Gestión_de_activos.

#Protección_de_la_información.

#Seguridad_de_los_recursos_humanos.

#Seguridad_física.

#Seguridad_del_sistema_y_de_la_red.

#Seguridad_de_las_aplicaciones.

#Configuración_segura.

#Gestión_de_identidad_y_acceso.

#Gestión_de_amenazas_y_vulnerabilidades.

#Continuidad.

#Seguridad_de_las_relaciones_con_los_proveedores.

#Cumplimiento_y_legal.

#Gestión_de_eventos_de¬_seguridad_de_la_información.

#Garantizar_la_seguridad_de_la_información.

e) Dominios de seguridad:

#Gobierno_y_ecosistema.

#Protección.

#Defensa.

#Resiliencia.

Con base en los atributos que se mencionan anteriormente, la ISO los presenta en una tabla, en la cual se informa qué tipo de atributos tiene ese control, lo que facilita comprenderlos mejor para poder desarrollarlos dentro de la empresa.

Por otra parte, también a la Norma se le establece algunos controles útiles para optimizar la eficiencia y funcionamiento correcto de la empresa, así como fomentar una mayor participación de los colaboradores y promover la cultura de mejora continua dentro de la organización; a continuación, se muestran los controles de importancia para la protección de los datos.

2.12 Control

Los controles tienen como objetivo asegurar la protección de cada activo, sistema, instalación, archivos y datos, con ayuda del departamento de TI, para realizar dentro la empresa, hace uso de uso de procedimientos y políticas,

previamente establecidos en la empresa, garantizando la confiabilidad, integridad y disponibilidad de todos los datos y los sistemas.

Estos suelen aplicarse en su totalidad o en parte, en la entidad, incluyendo la infraestructura y la plataforma de TI de la empresa que se auditó, para que se dé un funcionamiento correcto de los procesos.

2.13 Control físico

Francisco D. (2017) indica que “Consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial”. La ISO, en este dominio, incluyó dentro de la misma 14 controles, como guía para la desarrollarlas dentro de la empresa.

1. Perímetros de seguridad física.
2. Entrada física.
3. Aseguramiento de oficinas, salas e instalaciones.
4. Vigilancia de la seguridad física.
5. Protección contra amenazas físicas y ambientales.
6. Trabajar en áreas seguras.
7. Despejar escritorio y pantalla.
8. Emplazamiento y protección del equipo.
9. Seguridad de los activos fuera de las instalaciones.
10. Medios de almacenamiento.

11. Utilidades de apoyo.
12. Seguridad del cableado.
13. Mantenimiento del equipo.
14. Eliminación segura o reutilización de equipos.

Cada control perteneciente al dominio de control físico cuenta con propiedades y objetivos propios que facilitan su desempeño a la persona encargada de la implementación de los controles, así como el estudio de la seguridad de la empresa y el entendimiento de la función de ese control.

2.14 Perímetros de seguridad física

"Es utilizado para prevenir los accesos físicos no autorizados, daños e interferencias de la información de la organización y otros activos asociados" (ISO 27002, 2022, p. 67). Los perímetros de seguridad deben de encontrarse definidos dentro de la organización con el fin de mantener la protección de las áreas críticas de la empresa, como las encargadas de la manipulación y almacenamiento de archivos como de los demás activos.

2.15 Entrada física

"Se asegura de autorizar únicamente los puntos de acceso de información de la organización y de los demás activos asociados" (ISO 27002, 2022, p. 68). Se debe de mantener con medidas de protección las áreas donde solo al personal autorizado se le permite el ingreso, con el fin de evitar incidentes.

2.16 Aseguramiento de oficinas, salas e instalaciones

“Se asegura de prevenir accesos no autorizados, daños e interferencia a la información en organizaciones, oficinas, salas e instalaciones” (ISO 27002, 2022, p. 69). El aseguramiento de las distintas áreas de la infraestructura física de la empresa debe de encontrarse dividas de forma lógica, con la implementación de roles, para evitar que las actividades o la información confidencial se encuentren expuestas a cualquier persona.

2.17 Vigilancia de la seguridad física

“Su función es detectar y determinar los accesos no permitidos” (ISO 27002, 2022, p. 70). Las instalaciones deben de vigilarse de forma monótona, ya sea con la implementación de guardas de seguridad, durante todo el día, implementación de cámaras de vigilancia o demás herramientas físicas o tecnológicas, que permitan el manejo de ingreso de personas no autorizadas.

2.18 Protección contra amenazas físicas y ambientales

“Reducir o prevenir las consecuencias de los eventos originados de amenazas físicas y ambientales” (ISO 27002, 2022, p. 71). Es de importancia estar preparado ante cualquier amenaza, sea física o ambiental, mediante el estudio de riesgos a los que se encuentra expuesta la empresa, para tomar medidas preventivas y evitar que el incidente suceda o se convierta en un problema.

2.19 Trabajar en áreas seguras

“Se enfoca en la protección de la información y otros activos para aseguras las áreas de daños y accesos no autorizados de interferencias por trabajos del personal en esas áreas” (ISO 27002, 2022, p. 72). La supervisión de trabajos en las áreas de seguridad o informar al personal sobre las actividades que se vayan a realizar, corresponde a aspectos que se debe de tomar en consideración.

2.20 Despejar escritorio y pantalla

“Reducir el riesgo de accesos sin autorizar, perdida o daños de información en escritorios, pantallas y otras áreas de ubicaciones accesibles durante y fuera de las horas de trabajo” (ISO 27002, 2022, p. 73). En muchas ocasiones, al tratarse de equipo o áreas propias de trabajo, los trabajadores suelen descuidar la zona de trabajo o no tienen un manejo del espacio y con el paso del día, van acumulando información en los escritorios o monitores, sin tomar en cuenta que es un riesgo existente, para que las personas sin acceso puedan obtener dicha información.

2.21 Emplazamiento y protección del equipo

“Reducir el riesgo de amenazas físicas y del entorno, además de los accesos no autorizados y daño” (ISO 27002, 2022, p. 74). La protección del equipo físico es de importancia para la empresa, por lo cual, se debe mantener en lugares seguros, y con la implementación de ingresos por medio de roles para evitar incidentes por causa humana o natural.

2.22 Seguridad de los activos fuera de las instalaciones

“Prevención de perdida, daño, robo o comprometer de los dispositivos fuera de sitios e interrupciones de las operaciones de la organización” (ISO 27002, 2022, p. 75). Los dispositivos pertenecientes a la empresa o los dispositivos de propiedad de la persona colaboradora que realice el procesamiento de información, el cual se encuentre en las afueras de la infraestructura y se utilizan para funciones de la organización, deben de encontrarse protegidos en todo momento, para evitar incidentes.

2.23 Medios de almacenamiento

“Asegurar únicamente las autorizaciones de divulgación, modificación, eliminación o destrucción de la información almacenada de los medios” (ISO 27002, 2022, p. 76). Establecer políticas sobre la gestión de almacenamiento y la comunicación/capacitación de estas, deben de implementarse para que la información dentro de ella se encuentre segura en todo momento, en el ciclo de vida y adquisición por parte de la empresa.

2.24 Utilidades de apoyo

“Es la prevención de perdida, daños o comprometer la información y otros activos asociados, o interrupción de las operaciones de la organización debido al fallo y disrupción de las utilidades de apoyo” (ISO 27002, 2022, p. 77). La implementación de diferentes utilidades de apoyo, por medo de distintos proveedores, es de importancia para encontrarse protegido de cualquier fallo por parte de alguna utilidad de apoyo y así evitar problemas.

2.25 Seguridad del cableado

“Es la prevención de perdida, daños o comprometer la información y otros activos asociados, o interrupción de las operaciones relacionadas a energía y comunicación del cableado” (ISO 27002, 2022, p. 78). Aspectos como la instalación de cableado subterráneo o separación de cables de alimentación son pautas que se deben de considerar para comprometer información y mitigar daños.

2.26 Mantenimiento del equipo

“Es la prevención de perdida, daños o comprometer la información y otros activos asociados e interrupciones de las operaciones causadas por falta de mantenimiento” (ISO 27002, 2022, p. 79). El equipo de la empresa debe de encontrarse todo el tiempo disponible, manteniendo la integridad de la información y la confidencialidad, siendo importante que exista un área de mantenimiento dentro de la empresa y fechas programas cada cierto tiempo para la realización de las funciones.

2.27 Eliminación segura o reutilización de equipos

“Prevenir la falta de información de los equipos dispuestos o reusados” (ISO 27002, 2022, p. 80). Al hacer el cambio, desechar o reutilizar un equipo, se debe asegurar que la información se encuentre completa o no haya manera de poder obtenerla de nuevo.

2.28 Control tecnológico

Está conformada por un total de 34 controles, enfocado en la seguridad de la información resguardada a lo interno o en la nube.

1. Dispositivos de punto final de usuario.
2. Derechos de acceso privilegiado.
3. Restricción de acceso a la información.
4. Acceso a código fuente.
5. Autenticación segura.
6. Gestión de la capacidad.
7. Protección contra software malicioso.
8. Gestión de vulnerabilidades técnicas.
9. Gestión de la configuración.
10. Eliminación de información.
11. Enmascaramiento de datos.
12. Prevención de fuga datos.
13. Copia de seguridad de la información.
14. Redundancia de las instalaciones de procesamiento de información.
15. Registro.
16. Actividades de seguimiento.
17. Sincronización del reloj.
18. Uso de programas de utilidad privilegiadas.

19. Instalación de software en sistemas operativos.
20. Seguridad de las redes.
21. Seguridad de los servicios de red.
22. Segregación de redes.
23. Filtrado web.
24. Uso de la criptografía.
25. Ciclo de vida de desarrollo seguro.
26. Requisitos de seguridad de la aplicación.
27. Principios de arquitectura e ingeniería de sistemas seguros.
28. Codificación segura.
29. Pruebas de seguridad y aceptación.
30. Desarrollo subcontratado.
31. Separación de los entornos de desarrollo, prueba y producción.
32. Gestión de cambios.
33. Información de la prueba
34. Protección de los sistemas de información durante las pruebas de auditoría.

Cada uno de estos controles cuenta con objetivos y una guía que facilitan el entendimiento.

2.29 Dispositivos de punto final de usuario

“Para proteger la información contra los riesgos introducidos por el uso de dispositivos de punto final de usuario” (ISO 27002, 2022, p. 81). Se debe de

establecer políticas sobre configuración y manejo de los seguros de los dispositivos de punto final, comunicárselos a todos los trabajadores.

2.30 Derechos de acceso privilegiado

"Para garantizar que solo los usuarios autorizados, los componentes y servicios de software reciban derechos de acceso privilegiado" (ISO 27002, 2022, p. 83). Se trata de derechos de acceso que se conectan a una identidad o un rol dentro de la empresa, que les asignará a los trabajadores una serie de responsabilidades acorde con el nivel asignado.

2.31 Restricción de acceso a la información

"Para garantizar solo acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados" (ISO 27002, 2022, p. 85). El uso de las técnicas adecuadas de acceso dinámico, así como a diferentes tecnologías, serán capaces de respaldas la protección de los datos y garantizará un mayor control sobre ellos.

2.32 Acceso a código fuente

"Para evitar la introducción de funciones no autorizadas, evitar cambios no intencionales o maliciosos y mantener la confidencialidad de la propiedad intelectual valiosa" (ISO 27002, 2022, p. 86). Con un buen control del acceso a los códigos fuentes de los programas, la modificación o creación de copias, se convertiría en un riesgo bajo, dentro de la organización.

2.33 Autenticación segura

“Para garantizar que un usuario o una entidad se autentica de forma segura cuando se otorga acceso a sistemas, aplicaciones y servicios” (ISO 27002, 2022, p. 87). Contar con una autenticación correcta de los usuarios, al hacer ingreso en los sistemas o partes de las empresas, baja el nivel de riesgo de pérdida o modificación de datos, a uno inferior, pero para ello, es necesario hacer uso de técnicas adecuadas para que la tarea se realice de forma precisa.

2.34 Gestión de la capacidad

“Asegurar la capacidad requerida de las instalaciones de procesamiento de información, recursos humanos, oficinas y otras instalaciones” (ISO 27002, 2022, p. 89). Identificar de forma previa los requisitos mínimos de capacidad que permite las instalaciones que realizan el procesamiento de información, para no tener problemas a futuro por sobre carga de datos, también se debe de realizar una proyección de la capacidad que se va a requerir en un futuro cercano.

2.35 Protección contra software malicioso

Este tipo de protecciones sirven “para garantizar que la información y otros activos asociados estén protegidos contra programas malignos” (ISO 27002, 2022, p. 90). Existen programas malignos que afecta directamente al sistema operativo del dispositivo informático, por lo tanto, se requiere que la protección de los activos y la información se garantice de distintas maneras, mediante la instalación de programas de seguridad, una buena manipulación de los dispositivos finales y documentación por parte de los colaboradores de la empresa.

2.36 Gestión de vulnerabilidades técnicas

Son procedimientos que se utilizan “para prevenir la explotación de vulnerabilidades técnicas” (ISO 27002, 2022, p. 92). La empresa debe tener documentación sobre las vulnerabilidades técnicas a las que se encuentra expuesta, para proceder a evaluar le nivel de exposición ante ellas y poder desarrollar las medidas adecuadas para mitigarlas o eliminarlas.

2.37 Gestión de la configuración

“Para garantizar que el hardware, el software, los servicios y las redes funcionen correctamente con la configuración de seguridad requerida, y que la configuración no se altere por cambios no autorizados o incorrectos” (ISO 27002, 2022, p. 95). Se debe de documentar las configuraciones que se realizan en la empresa, tanto como las de seguridad, en dispositivos físicos, softwares, en servicios o en redes, además de monitorearse de forma constante, luego de la implementación, para revisiones y verificación del funcionamiento.

2.38 Eliminación de información

“Para evitar la exposición innecesaria de información confidencial y cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales para la eliminación de información” (ISO 27002, 2022, p. 97). Cuando la información almacenada en cualquier dispositivo físico deja de ser de utilidad, es importante que sea eliminada de forma adecuada y por completo, para evitar que cualquier persona acceda a ella.

2.39 Enmascaramiento de datos

“Para limitar la exposición de datos confidenciales, incluida la PII, y para cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales” (ISO 27002, 2022, p. 98). Se debe de hacer uso de acuerdo con la política que se específica en la organización con respecto al control del acceso, así como con las demás políticas que se encuentran relacionadas con el enmascaramiento de datos.

2.40 Prevención de fuga datos

“Para detectar y prevenir la divulgación y extracción no autorizada de información por parte de individuos o sistemas” (ISO 27002, 2022 p. 100). Las medidas contra fugas de datos deben implementarse en los sistemas, redes, dispositivos finales y todo aquel dispositivo que almacene o transfiera información confidencial.

2.41 Copia de seguridad de la información

“Para permitir la recuperación de la pérdida de datos o sistemas” (ISO 27002, 2022, p. 101). Las copias de seguridad deben de realizarse cada cierto tiempo, en un horario establecido y de preferencia en el momento cuando los servidores no se encuentren muy utilizados, para que la disponibilidad no se vea afectada.

2.42 Redundancia de las instalaciones de procesamiento

“Asegurar el funcionamiento continuo de las instalaciones de procesamiento de información” (ISO 27002, 2022, p. 102). La redundancia es un aspecto que no

se puede dejar de lado, para que la disponibilidad de los servicios se cumpla acorde con los requisitos solicitados.

2.43 Registro

“Para registrar eventos, generar evidencia, garantizar la integridad de la información de registro, prevenir el acceso no autorizado, identificar eventos de seguridad de la información que pueden conducir a un incidente de seguridad de la información y respaldar investigaciones” (ISO 27002, 2022, p. 103). Se debe de documentar todos los movimientos relacionados con las actividades dentro de la empresa, exceptuando las fallas y otros eventos de importancia.

2.44 Actividades de seguimiento

“Para detectar comportamientos anómalos y posibles incidentes de seguridad de la información” (ISO 27002, 2022, p. 106). Se deben de tomar medidas preventivas, con el fin de evaluar incidentes posibles de seguridad de los datos, por lo tanto, es relevante que las redes, sistemas y las aplicaciones que se utilizan, se encuentren monitoreadas para detectar comportamientos raros.

2.45 Sincronización del reloj

“Permitir la correlación y el análisis de eventos relacionados con la seguridad y otros datos registrados, y respaldar las investigaciones sobre incidentes de seguridad de la información” (ISO 27002, 2022, p. 108). Los relojes de los softwares de procesamiento de datos deben de encontrarse sincronizados con el horario local.

2.46 Uso de programas de utilidad privilegiadas

“Para garantizar que el uso de programas de utilidad no dañe el sistema y los controles de aplicaciones para la seguridad de la información” (ISO 27002, 2022, p. 109). Se debe de hacer uso de programas de utilidad que sean capaces de anular los controles del sistema, deben de restringirse de forma inmediata.

2.47 Instalación de software en sistemas operativos

“Para garantizar la integridad de los sistemas operativos y evitar la explotación de vulnerabilidades técnicas” (ISO 27002, 2022, p. 110). La implementación de procedimientos y medidas para una buena gestión de instalación de software es suma importancia, por lo tanto, se debe realizar desde fuentes confiables, con permisos del departamento de TI y asegurarse de que corresponda con lo solicitado.

2.48 Seguridad de las redes

“Para proteger la información en las redes y sus instalaciones de procesamiento de información de apoyo del compromiso a través de la red” (ISO 27002, 2022, p. 111). Se debe administrar y proteger los dispositivos de red y las redes como tal, para el control y protección de los sistemas.

2.49 Seguridad de los servicios de red

“Para garantizar la seguridad en el uso de los servicios de red” (ISO 27002, 2022, p. 112). Se debe de tener en consideración las características de seguridad,

los niveles de servicios, así como los requisitos y las medidas indispensables de seguridad.

2.50 Segregación de redes

"Dividir la red en límites de seguridad y controlar el tráfico entre ellos en función de las necesidades comerciales" (ISO 27002, 2022, p. 113). Se debe considerar la seguridad de las redes, mediante la división de dominios, para evitar el ingreso a páginas fraudulentas o que no son requeridas para las funciones de la empresa.

2.51 Filtrado web

"Para proteger los sistemas contra el programa maligno y evitar el acceso a sitios web no autorizados" (ISO 27002, 2022, p. 114). Se debe controlar el acceso a sitios externos maliciosos, por medio de técnicas de bloqueo de direcciones IP o dominios y así evitar los incidentes frecuentes.

2.52 Uso de la criptografía

La criptografía se utiliza para:

> Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad o la integridad de la información de acuerdo con los requisitos comerciales y de seguridad de la información, y teniendo en cuenta los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con la criptografía (ISO 27002, 2022, p. 115).

Se debe incluir la gestión de claves criptográficas, además de la definición e implementación de reglas para que se utilice eficazmente la criptografía.

2.53 Ciclo de vida de desarrollo seguro

"Garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo seguir de software y sistemas" (ISO 27002, 2022, p. 117). Es requerimiento fijar e implementar reglas para que sea una zona de desarrollo seguro, teniendo un lugar dentro de aplicaciones.

2.54 Requisitos de seguridad de la aplicación

"Para garantizar que todos los requisitos de seguridad de la información se identifiquen y aborden al desarrollar o adquirir aplicaciones" (ISO 27002, 2022, p. 118). Se debe identificar, determinar y luego aprobarse los requisitos de desarrollo o adquisición de aplicaciones.

2.55 Principios de arquitectura e ingeniería de sistemas seguros

"Garantizar que los sistemas de información se diseñen, implementen y operen de forma segura dentro del ciclo de vida del desarrollo" (ISO 27002, 2022, p. 120). Los principios de arquitectura e ingeniería deben estar detallados, documentados y, por supuesto, aplicados en las diferentes actividades relacionadas a los sistemas de información; la seguridad debe encontrarse acorde con cada capa de la arquitectura.

2.56 Codificación segura

“Garantizar que el software se escriba de forma segura. reduciendo así el número de posibles problemas de seguridad de la información” (ISO 27002, 2022, p. 122). Desde la parte de planificación como antes de la codificación, deben de encontrarse claros los principios que se deben de usar, tanto a nivel de un desarrollo nuevo o para la reutilización de aplicaciones.

2.57 Pruebas de seguridad y aceptación

“Para validar si se cumplen los requisitos de seguridad de la información cuando las aplicaciones o el código se implementan en el entorno de producción” (ISO 27002, 2022, p. 125). Se deben efectuar pruebas de seguridad de información, como actualizaciones, para asegurarse que cada mínimo detalle del proceso se efectué de forma adecuada.

2.58 Desarrollo subcontratado

“Para garantizar que las medidas de seguridad de la información requeridas por la organización se implementen en el desarrollo de sistemas subcontratados” (ISO 27002, 2022, p. 126). La empresa que subcontrató el servicio debe de encargarse de dirigir, vigilar y encargarse de revisar las diferentes actividades que están relacionadas con el desarrollo de este ámbito.

2.59 Separación de los entornos

“Para proteger el entorno de producción y los datos contra el compromiso de las actividades de desarrollo y prueba” (ISO 27002, 2022, p. 127). Se debe de contar con medidas y procedimientos con respecto a los diferentes entornos de trabajo, para evitar accesos no autorizados y evitar incidentes.

2.60 Gestión de cambios

“Preservar la seguridad de la información al ejecutar cambios” (ISO 27002, 2022, p. 128). Cada cambio que se realice en la infraestructura tecnológica de la empresa debe de informarse con antelación, para estar preparados ante las nuevas actualizaciones.

2.61 Información de la prueba

“Para garantizar la relevancia de las pruebas y la protección de la información operativa utilizada para las pruebas” (ISO 27002, 2022, p. 129). Se debe de seleccionar los informes de las pruebas que se efectúan y almacenarlas en lugares seguras con una adecuada gestión.

2.62 Protección de los sistemas de información

“Minimizar el impacto de la auditoría y otras actividades de aseguramiento en los sistemas operativos y procesos comerciales” (ISO 27002, 2022, p. 130). Para poder llevar a cabo una auditoría dentro de la empresa, debe de acordarse con tiempo, estableciendo una fecha y realizarla con tiempo, según lo que se acuerde con la gerencia de la empresa, como con la persona o empresa desarrolladora.

Capítulo III

Marco Metodológico

Marco metodológico

Se describen en este apartado, las técnicas y los métodos utilizados en este proyecto de investigación.

3.1 Enfoque

La investigación se desarrolla bajo el enfoque mixto, porque permite recopilar, analizar e integrar la información tanto de manera cualitativa como cuantitativa, logrando identificar aspectos con una mejor precisión y abordándolos desde diferentes puntos de vista.

Al requerirse diversos métodos y fuentes de datos para analizar los controles para la seguridad de la información implementados por la empresa Distribuidora COARSA, el enfoque utilizado debe facilitar el desarrollo y aplicación de técnicas e instrumentos para el proceso investigativo, tales como la revisión documental, las técnicas de análisis y recolección de datos que se requieren en este proyecto. Asimismo, “al realizar una investigación mixta, tanto de datos cuantitativos y cualitativos, el investigador gana amplitud y profundidad en la comprensión y corroboración, a la vez que compensa las debilidades inherentes del uso de cada enfoque por separado” (Aguilar, 2021, párr.9).

Por ende, se optó por este enfoque, porque la capacidad de análisis y versatilidad que brinda permite obtener información de una manera más completa al utilizar ventajas de ambos métodos, generando resultados más detallados, extensos y con una alta fiabilidad.

3.2 Tipo de investigación

Para cumplir con los objetivos planteados en este proyecto, se requiere aplicar varios tipos de investigación, el primero es la investigación de campo, porque será necesario realizar una serie de visitas a la empresa para identificar cómo se implementa el control físico y tecnológico en la empresa Distribuidora COARSA, se aplica este tipo investigación, porque “recopila los datos directamente de la realidad y permite la obtención de información directa en relación con un problema, apoyándose en informaciones que provienen entre otras, de entrevistas, cuestionarios, encuestas y observaciones” (Arias, 2020, párr.1).

Además, utilizando durante estas visitas, técnicas de recolección de datos como las citadas anteriormente, se logrará identificar cómo se implementa el control físico y tecnológico de la organización.

Por otra parte, se utilizará la investigación documental, porque esta se realiza “con base en revisión de documentos, manuales, revistas, periódicos, actas científicas, conclusiones y seminarios y /o cualquier tipo de publicación considerado como fuente de información” (Barahona, 2022, párr.12). Utilizar este tipo de investigación permitirá determinar lo establecido en la Norma ISO 27002, con respecto a los controles físicos y tecnológicos para la gestión de la seguridad de la información.

Igualmente, se necesita contrastar lo establecido por la Norma ISO 27002 con respecto al control físico y tecnológico, y las prácticas de control implementadas

en la empresa, por tanto, se hará uso de la investigación aplicada, dado que esta “busca la generación de conocimiento con aplicación directa a los problemas de la sociedad o el sector productivo, ocupándose del proceso de enlace entre la teoría y el producto” (Lozada, 2022, párr.1). Emplear este tipo de investigación permitirá desarrollar una política de seguridad para la organización, que posibilite atender los aspectos no documentados, relacionados con el control físico y tecnológico.

3.3 Población y muestra

La población, para efectos de esta investigación, está constituida por un total de 104 funcionarios, quienes tienen alrededor de más de cinco años de laborar con la empresa, además, están distribuidos por: ventas, gerencia, administración, facturación, recursos humanos, bodega, reparto y tecnologías de información.

La muestra será de 51 funcionarios, la cual se obtuvo mediante la fórmula matemática: tamaño de muestra = Z2 * (p) * (1-p) / c2. Utilizando un nivel de confianza del 95%, un margen de error de 10 y una población de 104 personas.

3.4 Técnicas de recolección de datos

Las técnicas e instrumentos que se utilizarán en esta investigación serán los siguientes.

3.4.1 Observación

Se usará para corroborar que se cumplan los controles físicos y tecnológicos y, además, para verificar cuáles de estos controles no se están cumpliendo, lo anterior mediante una serie de visitas a la organización.

3.4.2 Encuesta

Este instrumento se construirá con base en lo indicado en la Norma ISO 27002:2022, con respecto a los controles físicos y tecnológicos, constará de 15 preguntas relacionadas con el control físico y tecnológico, las cuales se aplicarán a la totalidad del personal de Tecnologías de Información y aproximadamente a 49 funcionarios de los demás departamentos, permitiendo identificar como se implementa este tipo de controles en la empresa Distribuidora COARSA o la falta de ellos.

3.4.3 Revisión documental

Se hará uso de una variedad de documentos y fuentes bibliográficas, entre ellas la Norma ISO 27002:2022, artículos, revistas y páginas web de confianza, con el propósito de determinar lo establecido en la Norma ISO 27002:2022, con respecto a los controles físicos y tecnológicos para la gestión de la seguridad de la información.

3.4.4 Lista de cotejo

Se desarrollarán dos listas de cotejo, una con base en los controles físicos, la cual contendrá aproximadamente 13 controles y la otra en el control tecnológico con aproximadamente 21 controles. Mediante este instrumento se logrará contrastar lo establecido en la Norma ISO 27002:2022 con respecto al control físico y tecnológico y las prácticas de control implementadas en la empresa Distribuidora COARSA.

3.4.5 Proceso de análisis y tabulación de datos

Una vez que se apliquen todos los instrumentos, se procederá a realizar el proceso de análisis y tabulación de los datos, mediante tablas y gráficos, utilizando los datos obtenidos tras la recopilación, con el fin de interpretar los resultados y desarrollar una política de seguridad para la empresa, de acuerdo con la Norma ISO 27002:2022, que les permita atender los aspectos no documentados, relacionados con el control físico y tecnológico en su organización.

3.5 Alcances y limitaciones

3.5.1 Alcances

El alcance de esta investigación será realizar un análisis del equipo físico y tecnológico de la empresa Distribuidora COARSA, haciendo uso de la Norma ISO 27002:2022, enfocándose en los capítulos VII y VIII de esta Norma, para un total de 34 controles que permitan el desarrollo de una política de controles físicos y tecnológicos para la organización.

3.5.2 Limitaciones

La investigación se limitará a analizar el control físico y tecnológico del equipo informático de la empresa Distribuidora COARSA, tomando como referencia la ISO 27002:2022, específicamente los capítulos VII y VIII relacionados con el control físico y tecnológico, que constan de un total de 48 controles de los cuales se utilizaran únicamente 34, debido a que no todos aplican para la empresa utilizada en esta investigación, cabe destacar que se utilizarán solamente los controles que el personal de Tecnologías de Información de la empresa y los investigadores

consideren necesarios. Los demás capítulos de la Norma no se tomarán en consideración. El periodo de recolección y análisis de datos para la investigación serán los primeros ocho meses del año 2023.

3.6 Preguntas generadoras

Se realizaron las siguientes preguntas generadoras para el desarrollo de esta investigación:

- ¿Cómo se implementa el control físico y tecnológico en la empresa Distribuidora COARSA?
- ¿Qué establece la Norma ISO 27002, con respecto a los controles físicos y tecnológicos, para la gestión de la seguridad de la información?
- ¿Qué tan apegadas están las políticas de seguridad de la empresa Distribuidora COARSA, con lo establecido en los capítulos VII y VIII de la Norma ISO 27002:2022?
- ¿Qué propuestas de mejora necesita la empresa Distribuidora COARSA en cuanto a controles físicos y tecnológicos, basados en la Norma ISO 27002:2022?

3.7 Cronograma

Tabla 1: Cronograma

Actividad	Fecha	Comentarios
Solicitud de documentación	31 de agosto, 2022	Se realiza la primera reunión con la empresa, para la solicitud de documentación sobre los controles tecnológicos que tienen en la empresa.
Análisis de la ISO 2700:2022	12 de setiembre, 2022. 19 de setiembre de 2022	Se procede con el estudio y el análisis de la ISO 27002:2022, tanto en sus controles físicos como tecnológicos.
Formulario de los controles físicos y tecnológicos	26 de setiembre, 2022 3 de octubre, 2022	Se realiza un formulario de los controles físicos y tecnológicos de la ISO 27002:2022, con el fin de identificar con ayuda de la empresa, los controles de mayor importancia.

Actividad	Fecha	Comentarios
Documentación de la empresa sobre los controles o medidas implementadas	10 de setiembre, 2022	El IT *manager* nos hace entrega de la documentación que poseen en la empresa.
Análisis de la documentación	12 de octubre, 2022	Se lee y analiza la documentación entregada.
Análisis de los resultados obtenidos del formulario	17 de octubre, 2022 24 de octubre,2022	Se lleva a cabo el análisis de los controles físicos y tecnológicos, para la identificación de aquellos que tienen un mayor grado de prioridad.
Lista de cotejo de los controles físicos	31 de octubre, 2022	Se realiza la primera lista de cotejo, para llevar a cabo la observación de los controles físicos que se implementan en la empresa.

Actividad	Fecha	Comentarios
Lista de cotejo de controles tecnológicos	7 de noviembre, 2022 14 de noviembre, 2022	Se realiza la segunda lista de cotejo, que se basa en los controles tecnológicos, para observar cuáles son ejecutados por la institución.
Realización de encuestas	21 de noviembre, 2022	Se formulan las preguntas para efectuarlas a la población seleccionada.
Reunión con el ITI Manager	24 de noviembre, 2022	Reunión con la empresa, para acordar las visitas para poder efectuar las listas de cotejo.
Revisión de listas de cotejo	28 de noviembre, 2022 5 de diciembre, 2022	Se revisan las listas de cotejo realizadas anteriormente, con el fin de poder efectuarlas de mejor manera.

Actividad	Fecha	Comentarios
	12 de diciembre, 2022	
Reunión con el ITI Manager	2 de enero, 2023	Se realiza una nueva reunión con el Manager de TI, de la entidad, para acordar las próximas visitas, para efectuar las listas de cotejo y las encuestas.
Consentimiento informado	4 de enero, 2023	Se redactan el documento para el consentimiento firmado, para poder hacer uso de las respuestas con fines académicos.
Primera visita a la empresa	11 de enero, 2023	Se realizan las primeras visitas, para poder llevar a cabo las listas de cotejo, por medio de la observación.
Segunda visita a la empresa	16 de enero, 2023	

Actividad	Fecha	Comentarios
Tercera visita a la empresa **Cuarta visita a la empresa**	17 de enero, 2023 18 de enero, 2023 19 de enero, 2023	Se inician con el llenado de las listas de cotejo de los controles tecnológicos, por medio de la observación.
Quinta visita a la empresa **Sexta visita a la institución**	20 de enero, 2023 21 de enero, 2023	Se realizan las últimas visitas a la institución, con el objetivo de efectuar las encuestas a la muestra del proyecto.
Tabulación de resultados de los controles físicos	23 de enero, 2023 30 de enero, 2023	Se tabulan los resultados obtenidos en las listas de cotejo de los controles físicos.
Tabulación de los resultados de los controles tecnológicos	06 de febrero 13 de febrero, 2023	Se procede con la tabulación de los resultados obtenidos en las listas de cotejo de los controles tecnológicos.

Actividad	Fecha	Comentarios
	20 de febrero, 2023	
Gráfica de las encuestas	13 de febrero, 2023	Se grafican y tabulan las respuestas obtenidas en las encuestas, dirigidas al personal de la empresa.
Mejora en las tabulaciones	20 de febrero, 2023 27 de febrero, 2023 06 de marzo, 2023	Se realizan mejoras en las tabulaciones de los datos recolectados, tanto de las listas de cotejo como de las encuestas.
Documentación	20 de marzo, 2023	Se actualiza el documento escrito, añadiendo los datos nuevos.
Manual de políticas	27 de marzo, 2023	Se investiga sobre la documentación de políticas en las empresas, así como el formato y el cuerpo.

Actividad	Fecha	Comentarios
Análisis de controles	10 de abril, 2023	Conforme con los resultados obtenidos en las listas de cotejo, se visualiza cuáles son aquellos controles con un bajo porcentaje.
Inicio de manual de políticas	17 de abril, 2023	Se comienza con la creación del manual de políticas de los controles físicos, basándonos en los que obtuvieron una nota baja.
Finalización de las políticas	19 de junio, 2023	Se finaliza la etapa de creación de las políticas físicas y tecnológicas
Se finaliza el proyecto.	20 de Julio, 2023	Se reciben todas las aprobaciones respectivas tanto de tutor y lectores, así como la carta de revisión por parte del filólogo.

3.8 Variables

Tabla 2:Variables o categorías de análisis

Variable	Definición conceptual	Definición operacional
Control físico	"Consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención, ante situaciones de amenazas a la información confidencial". (Directrices de Seguridad de la Información de la Universidad de Costa Rica, 2022, p. 1)	Medidas y barreras físicas utilizadas por la empresa COARSA para proteger la información confidencial ante situaciones de amenazas.
Control tecnológico	Son los controles que "utilizan la tecnología como una base para controlar el acceso y uso de datos confidenciales a través de una estructura física y sobre la red". (Generalidades sobre la seguridad, 2022, párr. 4)	Estructura física y sobre la red que utiliza la empresa COARSA para controlar el acceso y uso de datos confidenciales.
Norma	Una norma se denomina como una "regla que se debe seguir o a que se	Reglas que sigue la empresa COARSA para

Variable	Definición conceptual	Definición operacional
	deben ajustar las conductas, tareas, actividades, etc." (Real Academia Española, 2022, párr. 2)	gestionar tareas, conductas, actividades, etc.
ISO 27002	La Norma 27002 "es un estándar para la seguridad de la información que ha publicado la organización internacional de normalización y la comisión electrotécnica internacional". (Norma ISO 27002, 2022, párr. 1)	Estándar utilizado para verificar los controles físicos y tecnológicos en la empresa Distribuidora COARSA.
Gestión de la seguridad de la información	Son procedimientos y acciones que "permiten gestionar de manera adecuada la seguridad de la información institucional, a fin de hacer frente a amenazas de ataque o intromisión, error, actos fortuitos (inundación, incendio, etc.), entre otros". (Sistema de Gestión de Seguridad de la Información, 2022, párr.1)	Procedimientos y acciones utilizados por la empresa COARSA, para gestionar la seguridad de la información de la organización.

Variable	Definición conceptual	Definición operacional
Política de seguridad	La política de seguridad es “un conjunto de reglas, normas y protocolos de actuación que se encargan de velar por la seguridad informática de la empresa. Se trata de una especie de plan realizado para combatir todos los riesgos a los que está expuesta la empresa en el mundo digital”. (Caurin, 2018, párr.3)	Producto que se desarrollará con base en la Norma ISO 27002, que le permitirá a la empresa COARSA, poseer un conjunto de reglas, normas y protocolos que deberán seguir, para velar por la seguridad informática de la empresa.

3.9 Obstáculos y dificultades

Durante la elaboración del proyecto, se presentaron una serie de obstáculos y dificultades, los cuales se detallan a continuación.

- **Búsqueda de la empresa:** En ocasiones es un poco complicado conseguir una empresa que esté dispuesta a colaborar en este tipo de

proyectos relacionados con ciberseguridad, por la gran cantidad de información vulnerable que deben brindar, la empresa Distribuidora COARSA fue la excepción, nos brindaron los accesos necesarios de manera amable y atenta.

- **Transporte:** Al ser una empresa ubicada en San Ramón, los autores debieron desplazarse en reiteradas ocasiones desde Puntarenas, aumentando el nivel de dificultad del proyecto.
- **Horario laboral:** Muchas veces los horarios laborales de los estudiantes a cargo no permitían permanecer mucho tiempo en la empresa, lo cual los obligaba a volver varias veces a la organización para logar obtener los resultados deseados.
- **Disponibilidad del personal de TI:** En una organización que maneja tantos clientes, el personal de Tecnologías de Información siempre está ocupado, por esta razón se dificultó la programación de las citas con los colaboradores a cargo.

Capítulo IV

Presentación y análisis de resultados

Presentación y análisis de resultados

Se presentará en esta sección, un análisis detallado de los resultados obtenidos en la observación y la revisión documental. En primer lugar, para llevar a cabo una evaluación exhaustiva de la seguridad en las instalaciones de la organización, se empleó la técnica de la observación. Con la colaboración del personal de Tecnologías de la Información, se logró revisar minuciosamente cada área, identificando tanto los puntos vulnerables físicos como tecnológicos.

Gracias a esta técnica, se logró explorar detalladamente cada uno de los espacios, permitiendo tener una visión global de la situación y detectar cualquier posible riesgo o amenaza a la seguridad. Durante todo el proceso, se contó con el apoyo del personal especializado, lo que permitió que la evaluación se realizara rigurosa y efectivamente.

Una vez identificados los puntos vulnerables, se aplicaron listas de chequeo específicas para cada área, tanto físicos como tecnológicos, permitiendo una evaluación más precisa y detallada de la seguridad. De esta forma, se pudo determinar con mayor exactitud, los posibles riesgos y amenazas, así como las medidas necesarias para garantizar la seguridad y protección de las instalaciones.

A continuación, se llevó a cabo la revisión documental, la cual tuvo como objetivo examinar cada uno de los documentos de uso interno de la organización. Esta revisión permitió obtener información relevante y detallada sobre los

procedimientos y normas internas, junto con identificar áreas de mejora y posibles riesgos para la organización.

Gracias a esta revisión exhaustiva, se pudo obtener resultados significativos que contribuyeron a mejorar los procesos internos de la organización y a garantizar una mayor eficiencia y eficacia en su funcionamiento. Además, permitió detectar posibles errores o deficiencias en los documentos y procedimientos existentes.

Con respecto al “Manual de procedimientos operativos de análisis y estadística”, código “07.1-MP-01” de la empresa Distribuidora COARSA, se ha identificado que el objetivo principal del procedimiento de gestión de solicitudes de información es garantizar una gestión adecuada de las solicitudes de los usuarios, desde la recepción hasta la entrega final de la documentación. Para lograr este objetivo, se sigue un proceso que incluye la toma de requerimientos, análisis, retroalimentación, desarrollo y entrega de la documentación solicitada. Se ha evidenciado que es fundamental utilizar herramientas informáticas autorizadas por la empresa y sus socios comerciales, y se debe contar con autorización previa en algunos casos según lo establecido en la política TI-PO-07 de Seguridad de la Información.

El “Manual de procedimientos operativos de gestión de activos” tiene como objetivo llevar a cabo una correcta gestión de la entrega de activos, propiedad de la empresa, a los vendedores. El procedimiento se divide en varias etapas para asegurar un manejo adecuado y mantener los activos en buen estado.

El proceso comienza cuando el encargado(a) de Recursos Humanos informa sobre cualquier acción de personal relacionada con la gestión de activos. A continuación, se establece una comunicación fluida entre Recursos Humanos y el supervisor(a) encargado(a) de los vendedores. El siguiente paso implica el chequeo de los activos y el manejo de documentos y registros correspondientes.

La preparación de los documentos necesarios es responsabilidad del Departamento de Informática, en el cual los firman junto con el colaborador y el encargado(a) del departamento. Posteriormente, se realiza una revisión de los activos entregados, comparándolos con el *check list* previamente realizado en el momento de la entrega.

Si todo está en orden, se procede a actualizar el archivo digital y almacenar los activos en su lugar respectivo. Sin embargo, si se detecta algún problema, como daños o artículos faltantes, se informa al jefe inmediato y se envía un reporte a Recursos Humanos, adjuntando una cotización.

Con base en la información proporcionada, Recursos Humanos determina cómo proceder y el Departamento de Informática actualiza el archivo digital, registrando los cambios generados en torno al estado de los activos y su asignación.

Por otro lado, los resultados de la revisión documental del “Manual de procedimientos operativos de soporte técnico” tiene como objetivo detallar los pasos necesarios para gestionar una solicitud de soporte técnico, consultas y la adquisición de equipos informáticos. Para iniciar el proceso, el usuario puede

realizar una llamada o enviar un mensaje a través del correo electrónico o grupos de WhatsApp de soporte técnico correspondientes, solicitando asistencia en temas de TI o la adquisición de un equipo informático. Es importante destacar que, además de la comunicación verbal, se requiere que el usuario presente una solicitud por escrito para dejar constancia del requerimiento.

Cuando se trata de una solicitud de equipo informático, se evalúa el requisito técnico y la viabilidad para la empresa, verificando si el artículo está disponible en el inventario. Si se encuentra en *stock*, se procede con la entrega y se completan los formularios correspondientes. En caso contrario, se inicia la gestión para adquirir el artículo a través del proveedor de insumos, coordinando la logística junto con el encargado de bodega para asegurar su entrega.

En el caso de solicitudes de soporte técnico o consultas, el encargado del Departamento de Informática realiza un diagnóstico del problema para determinar si puede ser solucionado por el equipo interno de TI o si se requiere la intervención de un proveedor de servicios externo. Si la resolución puede realizarse internamente, se agenda una cita con el usuario para brindarle el soporte necesario. La prioridad de atención de cada caso es establecida por la Gerencia, considerando el impacto que pueda tener en los diferentes procesos del negocio.

El encargado de soporte técnico puede ofrecer asistencia a través de diferentes medios, como correo electrónico, WhatsApp, llamada telefónica, acceso remoto, utilizando herramientas como AnyDesk o TeamViewer, o incluso,

presencialmente. Sin embargo, para acceder de manera presencial o remota es necesario contar con la autorización previa del responsable del equipo y la presencia del usuario durante la asistencia técnica.

En situaciones cuando el encargado resuelva el problema, se proporciona una retroalimentación al usuario respecto al caso o si se tratara de una solicitud de equipo informático, se informa sobre la compra realizada. Si el encargado no puede solucionar el problema, se establece contacto con el proveedor para gestionar la situación. Finalmente, el encargado del Departamento de Informática mantiene una comunicación activa con el proveedor de servicios hasta que se haya resuelto completamente el caso, recibiendo retroalimentación por parte del proveedor.

A continuación, se presentan los resultados de la encuesta aplicada al personal de Distribuidora COARSA. La encuesta se realizó de manera aleatoria a colaboradores de distintas áreas de la empresa, incluyendo administración, jefatura, recepción, tesorería, bodega, reparto e inventario, con el propósito de obtener una perspectiva de la situación actual de la Institución desde el punto de vista de los trabajadores. Se buscaba evaluar el nivel de conocimiento del personal en temas de seguridad, debido a que son el primer equipo de protección para salvaguardar los activos de la empresa.

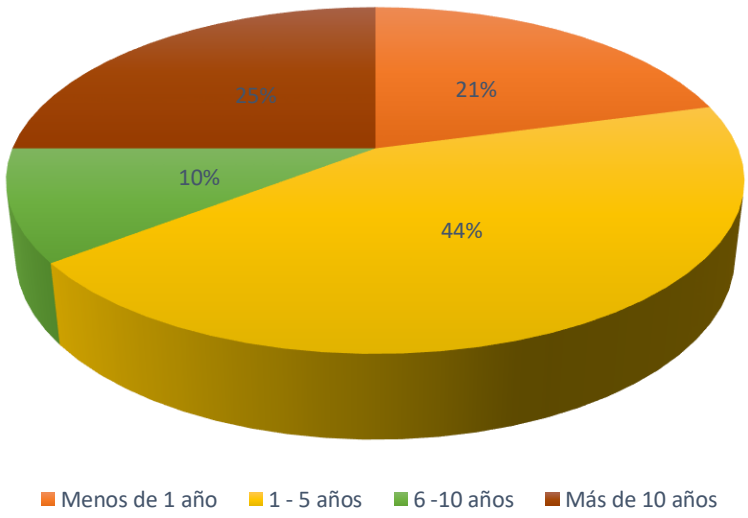
La encuesta contenía 15 preguntas de selección única y fue anónima para proteger la integridad de los colaboradores. Las opciones de respuesta no eran calificadas como correctas o incorrectas, dado que el objetivo era medir el nivel de

conocimiento del personal en temas de seguridad, tanto física como tecnológica. Las respuestas obtenidas fueron diversas, pero se observó una tendencia a la falta de capacitación en seguridad de la empresa, especialmente en lo que respecta al uso de dispositivos, el acceso a datos y la información o lugares clasificados. Este resultado se hizo más evidente entre los trabajadores nuevos.

Cabe destacar que existe una clara diferencia en el nivel de conocimiento en seguridad entre el personal de la parte administrativa y el de la bodega (inventario, reparto, etc.). Los colaboradores de estas últimas áreas, al consultarles sobre estos temas, evidencian menos conocimientos en aspectos de seguridad o información de la empresa.

Figura 1

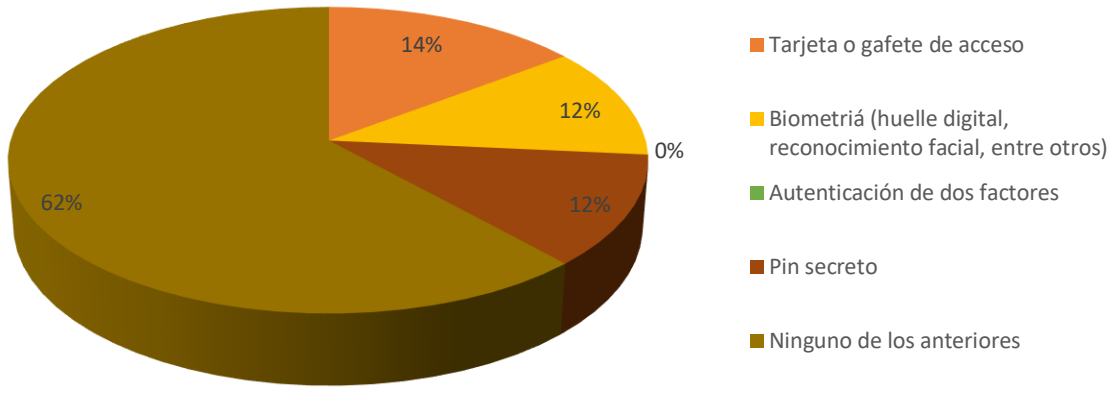
Distribución de la experiencia laboral del personal de COARSA



En el gráfico anterior se puede observar que la mayoría del personal de COARSA cuenta con una experiencia laboral de uno a cinco años en la organización. Esta información puede ser útil para la empresa al momento de evaluar la necesidad de capacitaciones y programas de retención de talento para los trabajadores más antiguos, así como para identificar oportunidades de crecimiento y promoción para aquellos con menor tiempo de servicio.

Figura 2

Mecanismos técnicos utilizados para el acceso a zonas restringidas

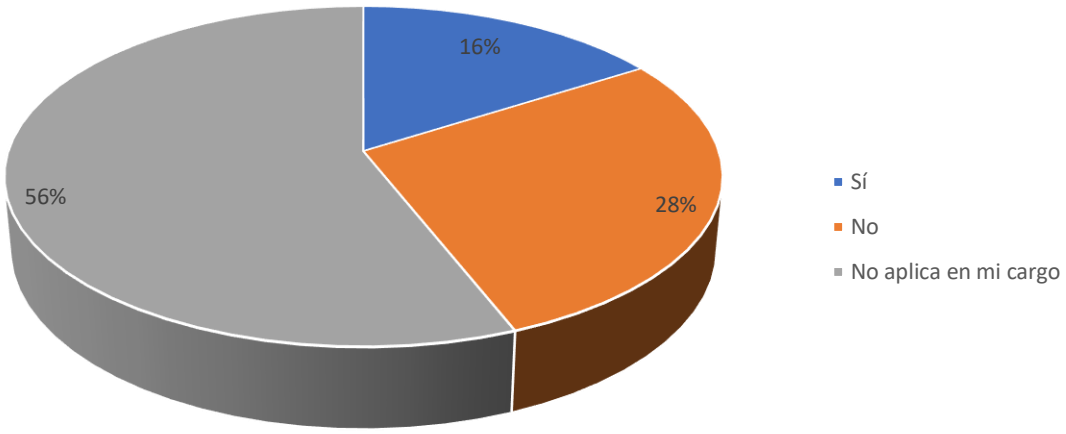


La gráfica muestra que una gran parte del personal de la organización no es sometida a ningún mecanismo de seguridad al momento de ingresar a la empresa. Esta situación puede resultar preocupante porque representa un riesgo potencial

para la seguridad de los activos de la organización. Es importante que la empresa evalúe la implementación de medidas de seguridad para garantizar la integridad de sus trabajadores y activos.

Figura 3

Registro y autenticación requeridos para acceder a información confidencial de la empresa: ¿Firma en libro físico o electrónico?

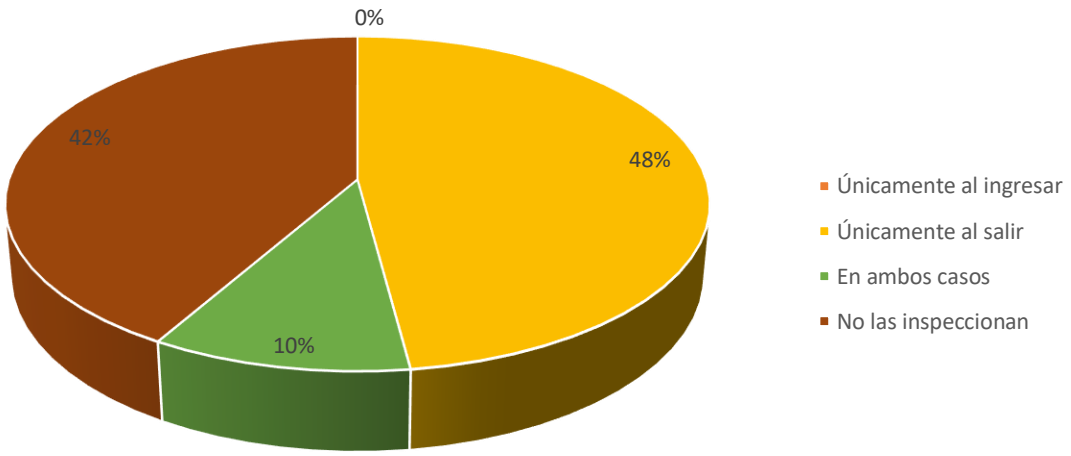


Se puede observar en el gráfico anterior que la mayoría del personal de la organización no requiere acceso a información confidencial, lo cual puede ser un indicio de que la empresa tiene políticas de seguridad bien establecidas para restringir el acceso a información sensible. Sin embargo, es preocupante que un porcentaje importante de los trabajadores indique que accede a información

confidencial sin tener que registrarse en ningún libro físico o electrónico, lo que sugiere que podría haber oportunidades para mejorar los mecanismos de control de acceso a información crítica.

Figura 4

Inspección de pertenencias al ingresar o salir de las instalaciones de la empresa: Percepción del personal

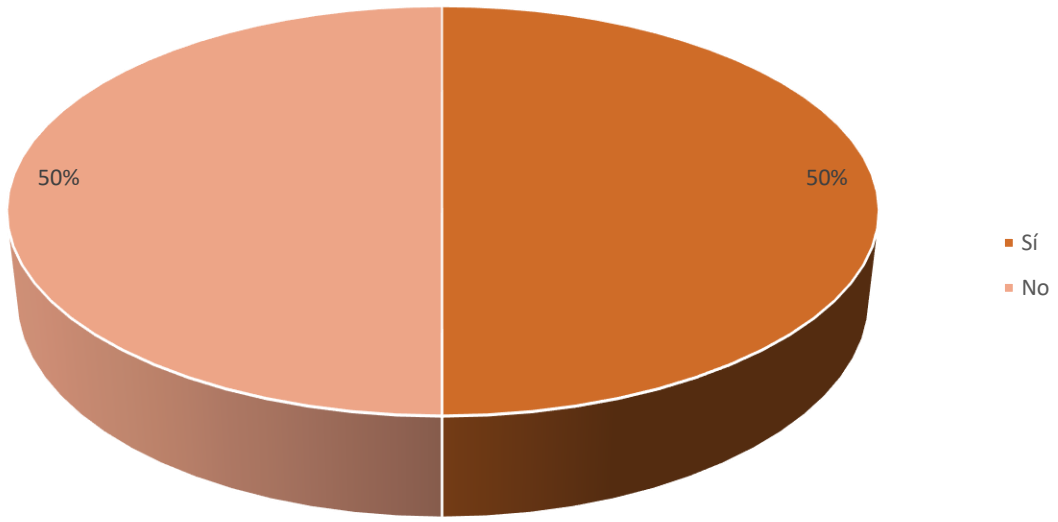


En el gráfico anterior se puede observar que la mayor parte del personal afirma que sus pertenencias son inspeccionadas únicamente al dejar las instalaciones, mientras que otro porcentaje importante afirma que no las inspeccionan.

En general, los resultados del gráfico sugieren que las medidas de seguridad en cuanto a la inspección de pertenencias no son uniformes en la organización. Es importante destacar que un porcentaje significativo de colaboradores afirmó que no se les realiza inspección alguna, lo que puede generar un riesgo para la seguridad de la empresa. Se sugiere que se realice una revisión y estandarización de las políticas de seguridad en cuanto a la inspección de pertenencias para garantizar la seguridad de la organización.

Figura 5

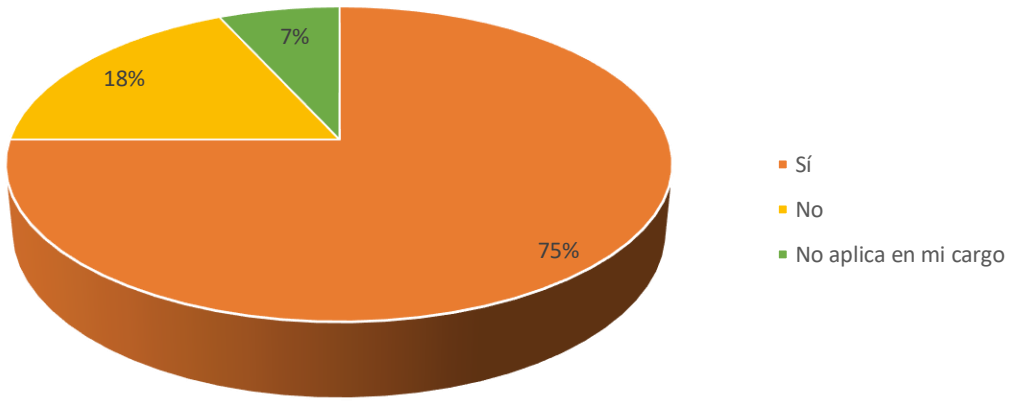
Uso de equipos de grabación durante la jornada laboral: Políticas y restricciones en la empresa



La gráfica anterior presenta una división en cuanto a la autorización para el uso de equipos de grabación durante la jornada laboral del personal de la organización. Es importante destacar que la mitad del personal no cuenta con este tipo de permisos, lo que puede ser indicativo acerca de la necesidad de establecer políticas claras en cuanto a la seguridad y privacidad de la información en la empresa.

Figura 6

Seguridad de los dispositivos electrónicos: Uso de contraseñas y bloqueo al abandonar el área de trabajo

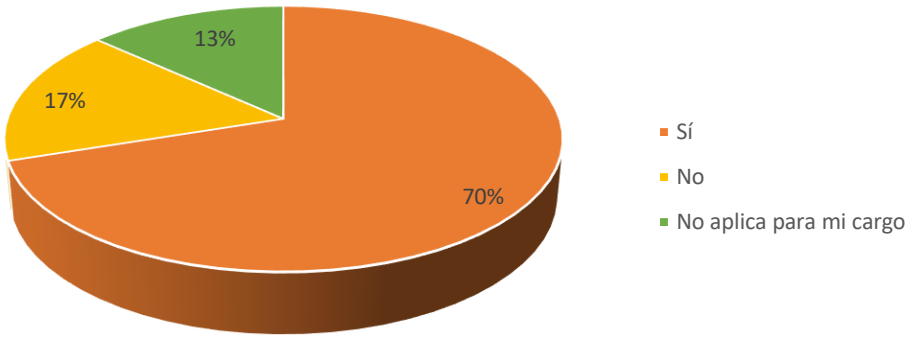


El gráfico anterior muestra que la mayoría del personal de la organización bloquea sus dispositivos electrónicos al abandonar su área de trabajo, lo cual indica una buena práctica de seguridad de la información. Sin embargo, hay un porcentaje

reducido que no lo hace o no aplica para su cargo, lo que sugiere la necesidad de reforzar la conciencia sobre la importancia de la seguridad de la información en la organización.

Figura 7

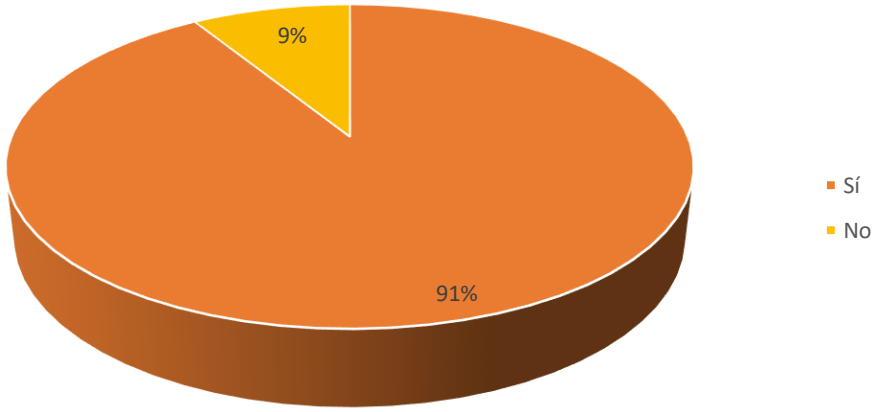
Manejo de información sensible en la oficina: Eliminación adecuada de datos escritos



La práctica de eliminar información sensible o confidencial anotada en pizarras antes de abandonar las instalaciones de la empresa es ampliamente adoptada por el personal de la organización, como se puede observar en el gráfico anterior. Empero, es importante destacar que un pequeño porcentaje aún no sigue esta práctica, lo que podría representar un riesgo potencial para la seguridad de la información de la empresa.

Figura 8

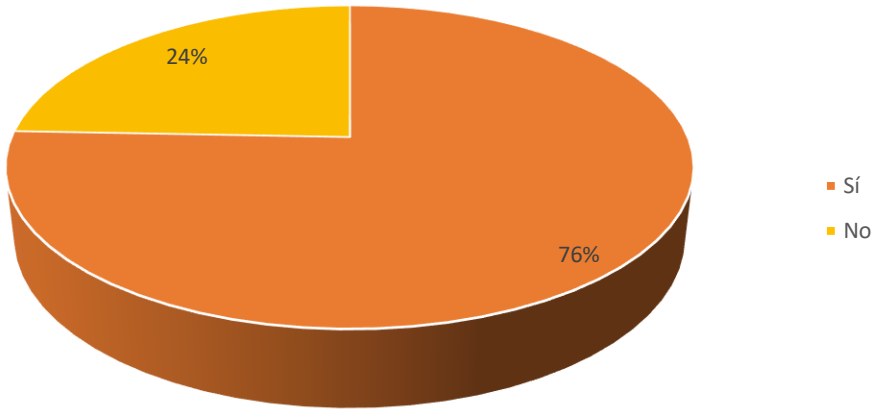
Regulaciones de alimentación, consumo de bebidas y tabaquismo en áreas cercanas a instalaciones de procesamiento de información: ¿Existen reglas establecidas por la empresa para comer, beber y fumar en las cercanías de las instalaciones?



En el gráfico anterior se observa que la mayor parte del personal tiene conocimiento acerca de las reglas establecidas por la empresa para comer, beber y fumar en las cercanías de las instalaciones donde se procesa información, mientras que un porcentaje muy reducido afirma que la organización no tiene este tipo de reglas.

Figura 9

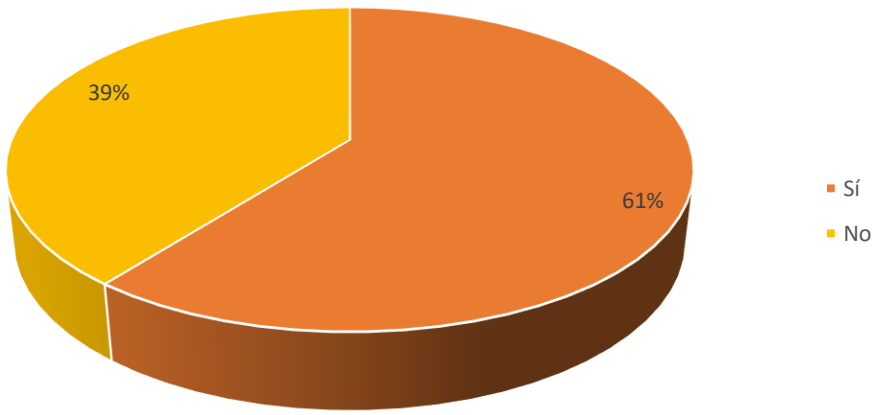
Políticas y reglas de uso de servicios y aplicaciones en Internet en la empresa: ¿La empresa cuenta con alguna política o reglas para el uso de servicios y aplicaciones en Internet?



En el gráfico anterior se puede observar que la mayoría del personal de la organización afirma que no existen reglas establecidas por la empresa para para el uso de internet. Pero un porcentaje muy reducido afirma que la organización si tiene este tipo de reglas, lo cual puede ser un factor de riesgo para la seguridad de la información, considerando que la mayoría no las usa o no tiene conocimiento de estas.

Figura 10

Reglas para la impresión de información en la empresa: ¿Al imprimir algún tipo de información debe de seguir ciertas reglas establecidas por la empresa?

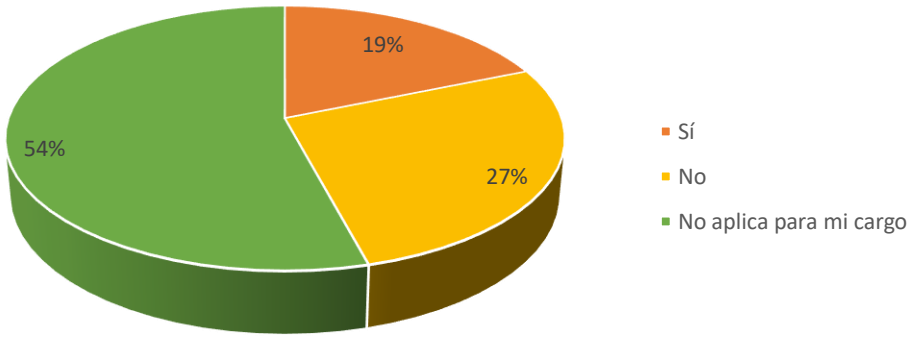


En el gráfico anterior, se puede observar que la mayoría del personal indica que existen reglas establecidas por la empresa para imprimir documentos, mientras que otro porcentaje importante afirma que no existe este tipo de pautas.

Los resultados muestran que existe cierto nivel de conocimiento y cumplimiento de las reglas establecidas por la empresa para imprimir documentos por parte del personal. Sin embargo, es importante destacar que una parte significativa del personal parece no estar al tanto de estas, lo que puede representar un riesgo potencial para la seguridad de la información.

Figura 11

Reglas y orientación para la configuración de ventanas emergentes en la empresa: ¿La empresa tiene establecidas reglas y orientación para la configuración de ventanas emergentes en las pantallas?



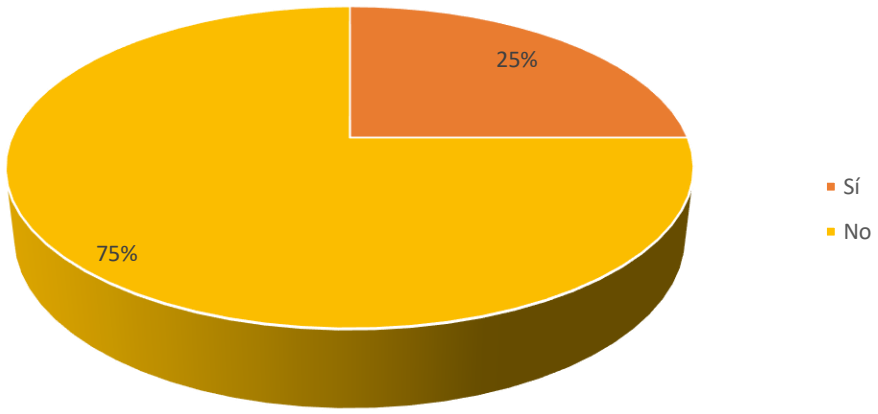
En el gráfico anterior se puede observar que la mayoría del personal indica que no es necesario o no se aplica el uso de reglas para la configuración de ventanas emergentes en las pantallas durante presentaciones, pantallas compartidas o en un área pública en sus cargos de trabajo, mientras que otro porcentaje niega la existencia de tales reglas en la organización. No obstante, una pequeña parte del personal afirma que la organización sí ha establecido este tipo de reglas.

Los resultados sugieren que la mayoría del personal no ha recibido instrucciones específicas en cuanto a la configuración de ventanas emergentes

durante presentaciones o en áreas públicas. Esto puede plantear preocupaciones en cuanto a la seguridad de la información, especialmente si se comparte información confidencial en pantallas compartidas o públicas.

Figura 12

Capacitación en la identificación y mitigación de amenazas de correo electrónico y archivos infectados: ¿Alguna vez ha recibido algún tipo de capacitación sobre cómo identificar y mitigar de forma potencial la recepción, envío o instalación de correos electrónicos, archivos o programas infectados?

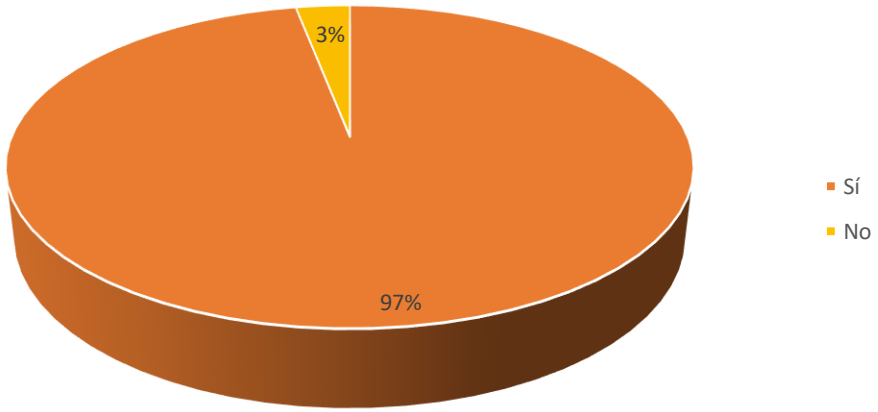


En la gráfica anterior se puede observar que la mayoría del personal de la organización no ha recibido capacitación sobre cómo identificar y mitigar el riesgo de recibir, enviar o instalar correos electrónicos, archivos o programas infectados. Pero un pequeño porcentaje afirma haber recibido este tipo de capacitación.

Los resultados sugieren que es necesario aumentar la conciencia y capacitación del personal en la organización sobre la importancia de la seguridad cibernética y cómo identificar y evitar amenazas potenciales para proteger la información y sistemas de la empresa.

Figura 13

Controles de seguridad para mitigar amenazas físicas y ambientales en la organización: ¿Conoce si la organización cuenta con controles para minimizar el riesgo de posibles amenazas físicas y ambientales, por ejemplo, robo, incendios, explosivos, humo, agua, entre otros?

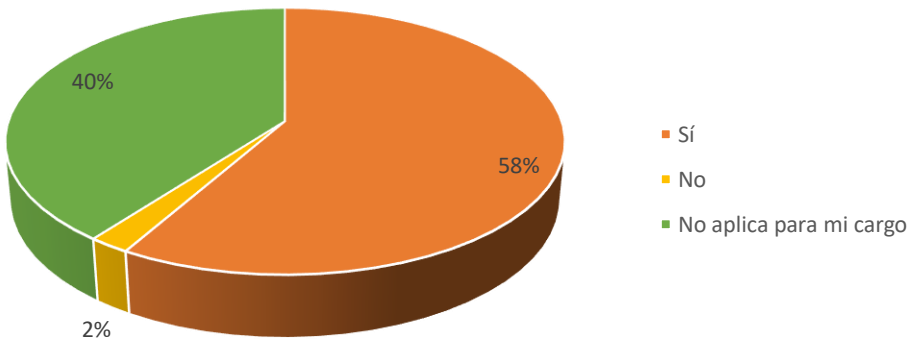


En el gráfico anterior se puede observar que la gran mayoría de los funcionarios de la empresa indica que esta cuenta con controles para minimizar el riesgo de posibles amenazas físicas y ambientales, tales como robo, incendios, explosiones, humo y agua.

Los resultados muestran que la organización ha tomado medidas de seguridad para minimizar el riesgo de posibles amenazas físicas y ambientales, lo cual es una buena práctica para garantizar la integridad de sus empleados y bienes.

Figura 14.

Procedimientos de autorización para el retiro de equipos y medios de las instalaciones de la organización: cuándo necesita retirar equipos y medios de las instalaciones de la organización, ¿se le solicita algún tipo de autorización?



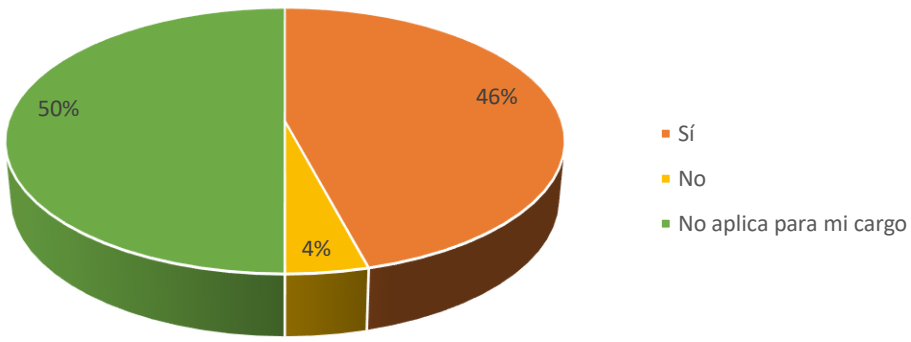
En el gráfico presentado se puede observar que la mayoría del personal afirma que se les solicita alguna forma de autorización al retirar equipos de la empresa, mientras que un porcentaje importante indica que no aplica para su cargo.

La autorización para retirar equipos de la empresa es un mecanismo importante de control de los recursos y la información. Se destaca como punto positivo que la mayoría del personal de la empresa tiene que seguir un proceso de

autorización antes de retirar cualquier equipo. Sin embargo, es necesario asegurar que estas políticas sean aplicables a todos los cargos y que se realice consistentemente para evitar cualquier riesgo potencial para la seguridad de la información.

Figura 15

Protección y seguridad de equipos y medios durante su retiro de las instalaciones de la organización: si por alguna razón requiere retirar un equipo o medio de almacenamiento de las instalaciones, ¿se asegura que este no quede desatendido o sin seguridad en sitios públicos?



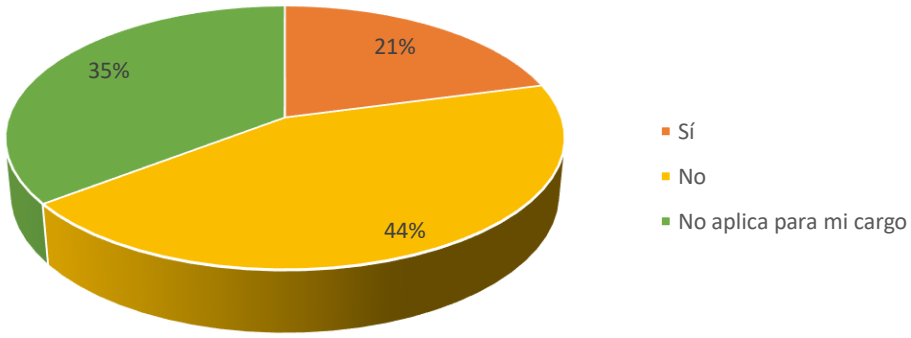
En el gráfico anterior se puede observar que un porcentaje significativo del personal afirma ser cuidadoso al retirar dispositivos de almacenamiento de la

organización, para evitar dejarlos desatendidos en público. No obstante, la mitad del personal señala que no requiere retirar este tipo de dispositivos de la empresa.

Estos resultados sugieren la importancia de establecer políticas y procedimientos claros sobre el manejo de dispositivos de almacenamiento y la seguridad de la información en la organización, para reducir el riesgo de posibles pérdidas o filtraciones de datos sensibles.

Figura 16

Uso de dispositivos de almacenamiento extraíbles en la computadora de trabajo: La computadora que utiliza para laborar ¿le permite el uso de dispositivos de almacenamiento extraíbles, tales como llaves mayas, discos duros externos, tarjetas SD o algún otro medio de almacenamiento?



En el gráfico anterior se puede observar que la mayoría del personal indica que sus computadoras tienen restricciones para el uso de dispositivos de

almacenamiento extraíbles, lo que puede indicar que la empresa ha implementado medidas de seguridad para prevenir la pérdida o filtración de información. Pese a que también es importante destacar que una parte no despreciable del personal afirmó que sí tiene permitido utilizar dispositivos extraíbles o que esta restricción no aplica para su cargo, lo que sugiere que se podría necesitar una revisión y actualización de las políticas de seguridad informática en la organización.

A continuación, se muestran los resultados obtenidos tras la aplicación de las listas de cotejo de controles físicos.

Tabla 3: Controles físicos

Política	Objetivo	Promedio de Puntos	Nivel de Cumplimiento
Perímetros de seguridad física	Evitar el acceso físico no autorizado, el daño y la interferencia a la información de la organización y otros activos asociados.	2	Medio
Entrada Física	Garantizar solo el acceso físico autorizado a la información de la	2	Medio

Política	Objetivo	Promedio de Puntos	Nivel de Cumplimiento
	organización y otros activos asociados.		
Seguridad de oficinas, salas e instalaciones	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información de la organización y otros activos asociados en las oficinas, salas e instalaciones.	3	Alto
Protección contra amenazas físicas y ambientales	Prevenir o reducir las consecuencias de eventos originados por amenazas físicas y ambientales.	2	Medio
Trabajar en áreas seguras	Proteger la información y otros activos asociados en áreas seguras contra daños e interferencias no autorizadas por parte del	2	Medio

Política	Objetivo	Promedio de Puntos	Nivel de Cumplimiento
	personal que trabaja en estas áreas.		
Escritorio y pantalla despejados	Reducir los riesgos de acceso no autorizado, pérdida y daño de la información en escritorios, pantallas y en otros lugares accesibles durante y fuera del horario normal de trabajo.	2	Medio
Ubicación y protección del equipo	Reducir los riesgos de amenazas físicas y ambientales, y de accesos y daños no autorizados.	2	Medio
Seguridad de los activos fuera de las instalaciones	Evitar la pérdida, el daño, el robo o el compromiso de los dispositivos externos y la interrupción de las operaciones de la organización.	3	Alto

Política	Objetivo	Promedio de Puntos	Nivel de Cumplimiento
Medios de almacenamiento	Garantizar solo la divulgación, modificación, eliminación o destrucción autorizadas de la información almacenada.	2	Medio
Utilidades de apoyo	Evitar la pérdida, el daño o el compromiso de la información y otros activos asociados o la interrupción de las operaciones de la organización debido a fallas e interrupciones de los servicios públicos de apoyo.	1	Bajo
Seguridad del cableado	Evitar la pérdida, el daño, el robo o el compromiso de la información y otros activos asociados y la interrupción de las operaciones de la organización relacionadas	3	Alto

Política	Objetivo	Promedio de Puntos	Nivel de Cumplimiento
	con el cableado de energía y comunicaciones.		
Mantenimiento de equipos	Evitar la pérdida, daño, robo o compromiso de la información y otros activos asociados y la interrupción de las operaciones de la organización causada por la falta de mantenimiento.	1	Bajo
Eliminación segura o reutilización de equipos	Evitar la fuga de información de los equipos que se desecharán o reutilizarán	2	Medio

Los resultados de la evaluación de cumplimiento de la empresa en cuanto a los controles físicos se encuentran detallados en la tabla 1. En relación con los perímetros de seguridad física, los edificios tienen perímetros sólidos, aunque algunas áreas, como la recepción, no cuentan con medidas de seguridad adecuadas. Las puertas y ventanas han sido debidamente aseguradas. No

obstante, no hay sistemas de alarmas contra incendios y aunque hay una brigada de emergencias, no se realizan inspecciones periódicas.

En cuanto a la entrada física, se ha constatado que el personal de seguridad solicita información personal para el acceso a la empresa y se otorgan identificaciones a todos los funcionarios. Además, se utilizan libros para control de acceso en áreas importantes. Al momento de la salida, se realiza una inspección a los vehículos, solicitando que se abran las ventanas y la cajuela. Con respecto a las entregas entrantes, la persona encargada no realiza inspecciones exhaustivas en busca de explosivos, debido a que consideran que no es necesario debido al tipo de mercancía que se recibe. Actualmente se realizan aproximadamente tres verificaciones.

La empresa cumple plenamente con la seguridad de oficinas, salas e instalaciones. Las zonas más críticas, el centro de datos y la zona de chequeo de mercancía, están ubicadas estratégicamente. El centro de datos cuenta con llave de seguridad, pero la puerta es de cristal transparente. Los funcionarios han manifestado su intención de cambiar el tipo de vidrio en el futuro. Las zonas críticas carecen de señalización, lo cual es recomendable según la norma ISO.

En cuanto a la protección contra amenazas físicas o ambientales, se ha constatado que la ubicación y construcción de las instalaciones son adecuadas. Se dispone de alarmas contra incendios que detectan eventos tempranamente, lo que protege los sistemas de información. Empero, no se realizan inspecciones aleatorias

para detectar armas o explosivos en vehículos o mercancías, lo que es necesario mejorar.

Por otra parte, los resultados indican que se está cumpliendo con las normas en lo que respecta al trabajo en áreas seguras, ya que se evita que se realicen labores sin supervisión en estas zonas, tanto por motivos de seguridad como para reducir las posibilidades de actividades maliciosas. Además, todas las zonas seguras se protegen con llaves y las zonas vacantes se mantienen bajo llave, permitiendo el acceso solo cuando sea necesario.

En relación con el escritorio y pantalla despejados, la empresa cumple con la mayoría de los controles, destacando la revisión de dispositivos cuando se produce un cambio de cargo, la configuración de las máquinas para que se bloqueen después de un tiempo sin actividad, el cambio de contraseñas caducadas y el almacenamiento seguro de documentos y medios extraíbles que contienen información confidencial.

En cuanto a la ubicación y protección de los equipos, se debe mejorar en aspectos como la protección contra rayos en las líneas eléctricas y de comunicaciones. Aunque se destaca que los equipos en ambientes industriales se encuentran debidamente protegidos, al igual que aquellos que procesan información y los sistemas están separados por áreas.

Respecto a la seguridad de los activos fuera de las instalaciones, se resalta la labor de los funcionarios para evitar que los dispositivos queden desatendidos en

zonas que se encuentran fuera de la empresa. Además, se utiliza una boleta para retirar o transportar los equipos y la autenticación de dos factores para su acceso. Es importante destacar que, en caso de robo de algún dispositivo, la empresa no tiene ningún mecanismo de borrado remoto, excepto el proporcionado por Google para los dispositivos móviles.

En lo que respecta al control de medios de almacenamiento, se observa que la empresa cumple parcialmente con los controles de este tipo y no cuenta con ninguna política específica sobre la gestión de estos medios. Sin embargo, el Departamento de Tecnologías de Información realiza procedimientos para proteger la información valiosa, tales como la realización de copias de seguridad, la desactivación de puertos USB en las máquinas de los funcionarios y la eliminación adecuada a través de empresas de confianza para prevenir la fuga de información y la entrada de programas maliciosos.

En cuanto a las utilidades de apoyo, la empresa no cumple con la mayoría de los controles. Por lo tanto, es importante trabajar en políticas que eviten la pérdida de información y activos asociados a la organización, cumpliendo con cada uno de los indicadores.

En lo que respecta a la seguridad del cableado, se cumple con la totalidad de los indicadores, lo que significa que el riesgo de pérdida, daño, robo o compromiso de la información y otros activos asociados con el cableado de energía y las comunicaciones es bastante bajo.

En cuanto al mantenimiento de equipos, se observa que es un aspecto que necesita reforzarse. Los resultados de este control muestran que la empresa no respeta la vida útil que indica cada fabricante de los equipos que utilizan y no cuenta con políticas de mantenimiento de equipos. A pesar de que la empresa tiene un plan remedial para controlar los fallos.

En lo referente a la eliminación segura o reutilización de equipos, los resultados indican un alto cumplimiento en los procesos de desecho de hardware. Empero, hay una excepción en el caso de las etiquetas que se deben utilizar en caso de donaciones a la beneficencia, tal como se indica en el anexo 1. Estas etiquetas no se utilizan porque la empresa no participa en este tipo de causas.

En resumen, la evaluación de cumplimiento de la empresa en cuanto a los controles físicos arrojó resultados mixtos. La empresa cumple con los controles en la seguridad de oficinas, salas e instalaciones, la ubicación y construcción de las instalaciones, el trabajo en áreas seguras, la ubicación y protección de los equipos, la seguridad del cableado y el control de medios de almacenamiento. No obstante, se necesitan mejoras en la seguridad de la entrada física, la protección contra amenazas físicas o ambientales, la protección contra rayos en las líneas eléctricas y de comunicaciones, la seguridad de los activos fuera de las instalaciones, las utilidades de apoyo y el mantenimiento de equipos. La empresa debe trabajar en políticas que eviten la pérdida de información y activos asociados a la organización y cumplir con cada uno de los indicadores del anexo 1 para mejorar su cumplimiento

en seguridad física. A continuación, se muestran los resultados obtenidos tras la aplicación de las listas de cotejo de controles tecnológicos.

Tabla 4: Controles tecnológicos

Política	Objetivo	Promedio de Puntos	Nivel de Cumplimiento
Dispositivos de punto final	Proteger la información contra los riesgos introducidos por el uso de dispositivos de punto final de usuario.	2	Medio
Derechos de acceso privilegiado	Garantizar que solo los usuarios autorizados, los componentes y servicios de software reciban derechos de acceso privilegiado.	2	Medio
Restricción de acceso a la información	Garantizar solo el acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados.	2	Medio

Política	Objetivo	Promedio de Puntos	Nivel de Cumplimiento
Acceso al código fuente	Evitar la introducción de funciones no autorizadas, evitar cambios no intencionales o maliciosos y mantener la confidencialidad de la propiedad intelectual valiosa.	1	Bajo
Autenticación segura	Garantizar que un usuario o una entidad se autentica de forma segura cuando se otorga acceso a sistemas, aplicaciones y servicios.	2	Medio
Protección contra software malicioso	Garantizar que la información y otros activos asociados estén protegidos contra *malware*	2	Medio

Política	Objetivo	Promedio de Puntos	Nivel de Cumplimiento
Gestión de vulnerabilidades técnicas	Prevenir la explotación de vulnerabilidades técnicas.	1	Bajo
Gestión de la configuración	Garantizar que el hardware, el software, los servicios y las redes funcionen correctamente con la configuración de seguridad requerida y que la configuración no se altere por cambios no autorizados o incorrectos.	2	Medio
Eliminación de información	Evitar la exposición innecesaria de información confidencial y cumplir con los requisitos legales, estatuarios y reglamentarios y	2	Medio

Política	Objetivo	Promedio de Puntos	Nivel de Cumplimiento
	contractuales para la eliminación de información.		
Prevención de fuga de datos	Detectar y prevenir la divulgación y extracción no autorizada de información por parte de individuos o sistemas.	3	Alto
Copias de seguridad de la información	Permitir la recuperación de la pérdida de datos o sistemas.	3	Alto
Redundancia de las instalaciones de procesamiento de información	Asegurar el funcionamiento continuo de las instalaciones de procesamiento de información.	3	Alto
Registro	Registrar eventos, generar evidencia, garantizar la integridad de la información		

Política	Objetivo	Promedio de Puntos	Nivel de Cumplimiento
	de registro, prevenir el acceso no autorizado, identificar eventos de seguridad de la información que pueden conducir a un incidente de seguridad de la información y respaldar investigaciones.	2	Medio
Actividades de seguimiento	Detectar comportamientos anómalos y posibles incidentes de seguridad de la información.	3	Alto
Instalación de software en sistemas operativos	Garantizar la integridad de los sistemas operativos y evitar la explotación de vulnerabilidades técnicas.	3	Alto
Seguridad de redes	Proteger la información en las redes y sus instalaciones	3	Alto

Política	Objetivo	Promedio de Puntos	Nivel de Cumplimiento
	de procesamiento de información de apoyo del compromiso a través de la red.		
Seguridad de los servicios de red	Garantizar la seguridad en el uso de los servicios de red.	2	Medio
Segregación de redes	Dividir la red en límites de seguridad y controlar el tráfico entre ellos en función de las necesidades comerciales	3	Alto
Filtrado web	Proteger los sistemas contra el *malware* y evitar el acceso a sitios web no autorizados.	1	Bajo
Separación de los entornos de desarrollo,	Proteger el entorno de producción y los datos contra el compromiso de las		

Política	Objetivo	Promedio de Puntos	Nivel de Cumplimiento
prueba y producción	actividades de desarrollo y prueba.	2	Medio
Gestión de cambios	Preservar la seguridad de la información al ejecutar cambios.	2	Medio

Los resultados de la evaluación de cumplimiento se encuentran detallados en la tabla 2. En relación con los dispositivos del punto final, la empresa cuenta con un nivel de cumplimiento medio. Por un lado, existen registros de los dispositivos por número de serie y propietario, pero, por otro lado, no se cumplen los requisitos para la protección física. Es importante destacar que a nivel de *active directory*, la empresa cuenta con una serie de restricciones que prohíben la instalación de software. Empero, se detectó un aspecto negativo: la falta de cifrado en los dispositivos extraíbles, lo cual va en contra de lo que indica la norma ISO para proteger la información contra los riesgos asociados al uso de dispositivos de punto final del usuario. A pesar de esto, un punto positivo es que la empresa cuenta con protección contra programas malignos mediante el software de pago Eset End Point Security. Además, se realizan copias de seguridad tanto a nivel de servidores como en dispositivos extraíbles. También se bloquea el uso de los puertos USB en todos

los dispositivos. Por otro lado, es importante mencionar que la Norma indica que los dispositivos deben bloquearse al abandonar el puesto de trabajo, lo cual la empresa cumple en su totalidad. Sin embargo, se identificó un aspecto importante: la empresa no cuenta con las respectivas licencias de Windows 10 para la totalidad de los equipos, lo cual constituye un incumplimiento grave de la Norma. En resumen, con respecto a los dispositivos de punto final, la empresa cumple parcialmente.

Con respecto a los derechos de acceso privilegiado, los resultados fueron bastante satisfactorios, porque la empresa cumple casi la totalidad de los controles indicados por la norma. No obstante, hay dos aspectos en los que no se hace: la implementación de requisitos para el vencimiento de los derechos de acceso privilegiado y las revisiones constantes a los usuarios que poseen este tipo de permisos.

En el caso de la restricción de acceso a la información, se detectó que la organización no cumple con varios controles de la norma. Por ejemplo, no se guarda el registro de cambios que se efectúan, lo cual es crucial para investigaciones futuras. En resumen, la empresa aún debe mejorar en estos aspectos si desea cumplir con lo indicado en la Norma y garantizar que solo los usuarios autorizados, los componentes y servicios de software reciban derechos de acceso privilegiado. A pesar de esto, el cumplimiento por parte de la empresa es alto.

En cuanto al acceso al código fuente, los resultados fueron bastante preocupantes, dado que la empresa no cuenta con procedimientos establecidos para la administración y el acceso a los códigos fuente. Aunque se manipulan más bases de datos, no tienen una protección para denegar el acceso directo a los repositorios de código fuente. Además, no se mantiene un listado de programas en un entorno seguro en el que los procesos de lectura y escritura puedan ser asignados y administrados. Esto implica la falta de un registro para el caso de ser necesaria una auditoría.

En relación con la autenticación segura, la empresa cumple de manera parcial, es decir, obtuvo un nivel medio. Algunos de los aspectos que no se cumplen son la falta de avisos en las instalaciones que indiquen que solo el personal autorizado puede ingresar a ciertas áreas, el inicio de sesión sin mensajes específicos de ayuda, la protección contra intentos de inicio de sesión de fuerza bruta y el registro de intentos fallidos. En resumen, la empresa debe mejorar en los aspectos anteriores, si desea garantizar que un usuario o entidad se autentique de forma segura cuando se le otorga acceso a sistemas, aplicaciones y servicios.

En lo referente a la protección contra software malicioso, la empresa no cumple con las medidas de seguridad contra los riesgos asociados con la obtención de archivos tanto de redes externas u otros medios, los procedimientos para el tratamiento de software malicioso ni ningún tipo de capacitación de uso. Los resultados indican que la empresa cumple parcialmente, pero aún no es capaz de

garantizar que la información y otros activos asociados estén protegidos contra programas malignos.

En cuanto a la gestión de vulnerabilidades técnicas, la empresa no cumple con la mayor parte de indicadores de la Norma, como el establecimiento de funciones y responsabilidades asociados a la gestión técnicas de vulnerabilidades, creación y actualización de listas de acuerdo con los cambios que se hagan en el inventario o en el caso de que existan recursos nuevos o útiles, así como el abordaje de vulnerabilidades basados en procedimientos de respuestas a incidentes de seguridad de la información. En este control, la empresa debe mejorar bastante si quiere estar preparada para prevenir la explotación de vulnerabilidades técnicas.

En lo que concierne a la gestión de la configuración, la empresa cumple con la mayoría de los indicadores, pero debe mejorar en el control de identidades que ya no se utilizan en los equipos y la verificación de licencias que es un aspecto que se mencionó anteriormente, la empresa no cuenta con licencias del sistema operativo Windows 10. Lo anterior, con el fin de garantizar que el hardware, el software, los servicios y las redes funcionen correctamente con la configuración de seguridad requerida.

Respecto al control de eliminación de la información, la empresa obtuvo un nivel de cumplimiento medio, a pesar de que se registra cada resultado de eliminación de información, no se utiliza algún tipo de software que garantice que la información no pueda ser recuperada, lo cual incumple con lo estipulado en la

Norma en dicho control, además, no utilizan proveedores aprobados y certificados, porque la eliminación se realiza por el mismo personal de Tecnologías de Información de la empresa, cabe destacar que los mecanismos de eliminación se utilizan de acuerdo con el medio de almacenamiento.

Por otra parte, con respecto al control de prevención en fuga de datos, la empresa, la organización obtuvo un nivel de cumplimento bastante alto; no obstante, los funcionarios afirman que aún existen ciertas vulnerabilidades que deben tratarse.

En el caso del control de copias de seguridad de la información, la empresa obtuvo resultados muy similares a los del control anterior, cumplimiento con la mayoría de los indicadores de la Norma, a excepción del caso de la encriptación de las copias de seguridad que se almacenan, porque no se utiliza ningún tipo de encriptación, lo cual es lo contrario a lo que indica la Norma.

Así mismo, con respecto a la redundancia de las instalaciones de procesamiento de información, la organización cumple con la mayor parte de los indicadores de la Norma, a excepción de la redundancia de las fuentes de alimentación físicas, porque únicamente se utiliza el ICE.

En lo que concierne al control de registro de eventos, la empresa obtuvo un nivel medio, cumpliendo con una parte importante de los controles, a excepción de la creación, modificación y eliminación de identidades, dado que no se guarda esa información, tampoco se cuenta con un plan en caso de fallar el registro de eventos

o que se sobrescriban eventos del pasado; otro aspecto importante es que no se cuenta con una lista de excepciones identificadas previamente, mediante el uso de reglas predeterminadas, no se examinan los informes de uso de los proveedores de servicios ni se incluyen los registros de eventos de monitoreo físico.

En cuanto al control de actividades de seguimiento, los resultados indican un nivel de cumplimiento bastante alto, la organización cumple total o parcialmente con la mayoría de los indicadores de la Norma, a excepción de la verificación de intentos fallidos en accesos a los recursos protegidos, lo cual es un aspecto importante que exige la ISO.

En lo que respecta al control de instalación de software en sistemas operativos, la organización cumple con la mayor parte de los indicadores de la Norma, a excepción de los registros de auditoría de todas las actualizaciones del sistema operativo, que es algo que no se realiza en la empresa.

En relación con la seguridad de redes, la organización se destacó en la mayor parte de los indicadores, a excepción de la falta de controles para salvaguardar la confiabilidad, que a como indica la Norma, son necesarios para proteger las aplicaciones y los sistemas conectados, además, no existe un registro y seguimiento adecuado para permitir la grabación y detección de acciones que puedan afectar la seguridad de la información.

Igualmente, los resultados obtenidos en el control de seguridad de los servicios de red, indican un nivel de cumplimiento medio, debido a que no existen

requisitos de autenticación para acceder a diversos servicios de red, no existen procedimientos de autorización para determinar a quién se le permite acceder a ciertas redes, no se tiene gestión de la red, controles, ni procedimientos tecnológicos para proteger el acceso a la red, ni se implementan registros de horas, ubicación, ni otros atributos del usuario al momento del acceso, además, no existen parámetros técnicos para la conexión segura de los servicios de red, de acuerdo con las normas de seguridad y conexión de red; asimismo, tampoco existen procedimientos para el uso de servicios de red que permitan restringir el acceso a servicios o aplicaciones de red, tal y como lo indica la Norma.

Con respecto al control de segregación de redes, los resultados indican que la organización cumple con la mayor parte de los indicadores de la Norma, a excepción del uso de políticas específicas sobre el control, requisitos de acceso, el valor y la clasificación de la información procesada.

Por otra parte, en el caso del control y filtrado web, los resultados fueron bastante lamentables, porque la empresa no está cumpliendo con la totalidad de los indicadores de la Norma, es decir, que se permite el acceso a sitios web sospechosos o maliciosos, no hay servidores de mando y control, a pesar de que la organización cuenta con un *firewall* con capacidad, no está configurado totalmente, por lo tanto, no se aprovecha.

En lo que respecta al control de la separación de los entornos de desarrollo de prueba y producción, los resultados indican un nivel de cumplimiento medio, por

una parte no se hace una correcta separación de los sistemas de desarrollo y producción ni se definen o documentan autorizaciones para el despliegue de software del estado de desarrollo al estado de producción, pero en el caso de otros indicadores si se observan resultados positivos, como el seguimiento en los cambios del entorno y en la realización de copias de seguridad.

En cuanto a la gestión de cambios, los resultados indican un nivel de cumplimiento medio, entre los indicadores que destacan, se encuentran las pruebas y su respectiva aceptación en el caso de cambios.

Con respecto a los indicadores con resultados bajos o inexistentes, se encuentran, la inadecuada planificación y evaluación del impacto potencial de los cambios, considerando todas las dependencias, así como la falta de planes de implementación y procedimientos de respaldo, incluidas las consideraciones de emergencia.

Capítulo V

Diseño e implementación del proyecto

Diseño e implementación del proyecto

En este proyecto en particular, es importante destacar que el enfoque se diferenció de los métodos convencionales de diseño y desarrollo. Al tratarse de una serie de documentos dirigidos a la empresa, se evitó el camino tradicional de crear productos tangibles o programas de software. En su lugar, se le dio prioridad a la creación de políticas de seguridad física y tecnológica. Estas políticas se convierten en un conjunto de directrices vitales para proteger los activos de la organización y asegurar su funcionamiento continuo. Al considerar tanto la documentación interna de la empresa como las pautas establecidas en la norma ISO 27002:2022, se buscó establecer un puente que conectara los valores fundamentales de la organización con los estándares de seguridad reconocidos a nivel internacional.

En cuanto a la perspectiva de la implementación, la investigación fue cuidadosamente diseñada para concentrarse en la formulación de estas políticas. Sin embargo, es crucial tener en cuenta que estas políticas no solo son palabras, sino un reflejo de los valores y la cultura de la organización. Aunque no se consideró parte esencial del proyecto llevar a cabo la implementación práctica, es importante mencionar que esta etapa constituye un paso clave en la dirección de fortalecer la seguridad en la empresa. La decisión de si se adoptarán estas políticas y cómo se adaptarán a la realidad operativa queda completamente en manos de la empresa, que podrá tomar esta determinación basándose en sus necesidades específicas y sus objetivos estratégicos.

En última instancia, el proyecto proporcionó un marco sólido para la seguridad y la protección de la empresa, mientras otorgaba a la misma la libertad de definir su futuro en materia de ciberseguridad.

Capítulo VI

Conclusiones y recomendaciones

Conclusiones y recomendaciones

6.1 Conclusiones

Se concluye lo siguiente, con base en el análisis de los controles para la seguridad de la información, basado en la Norma ISO 27002:2022.

- La técnica de observación resultó ser una herramienta fundamental para llevar a cabo una evaluación rigurosa y detallada de la seguridad en las instalaciones de la organización.
- La revisión documental permitió obtener información relevante y detallada sobre los procedimientos y normas internas, así como también identificar áreas de mejora y posibles riesgos para la organización.
- La selección previa de los controles incluidos en el proceso de análisis fue de gran utilidad para priorizar los esfuerzos en las áreas más vulnerables de la organización.
- Durante el análisis se han encontrado ciertas disparidades entre las prácticas actuales de control físico y tecnológico de Distribuidora COARSA y los requisitos establecidos en la Norma ISO 27002:2022.
- La identificación de discrepancias ha permitido identificar áreas específicas en las que Distribuidora COARSA puede mejorar sus controles físicos y tecnológicos. Esto puede implicar el fortalecimiento de la seguridad de las instalaciones, la implementación de medidas adicionales para proteger los activos de información, la revisión y mejora de los procedimientos de gestión

de riesgos y el establecimiento de un enfoque más robusto para la respuesta a incidentes de seguridad.

- El análisis de datos es fundamental para identificar incongruencias y áreas de mejora en los controles físicos y tecnológicos, permitiendo detectar patrones y brechas en la seguridad, siendo crucial para una gestión más efectiva y objetiva de la seguridad de la información.
- Se ha trabajado en el fortalecimiento de las políticas de seguridad, las cuales se han desarrollado de acuerdo con las necesidades de la organización. Estas políticas se encuentran detalladas en la sección de anexos.

6.2 Recomendaciones

Una vez concluida la investigación se sugiere lo siguiente.

- Se recomienda que la Organización implemente los controles establecidos en la Norma ISO 27002:2022, prestando especial atención a los capítulos VII y VIII, que abordan los controles físicos y tecnológicos para proteger los sistemas de información.

- Es necesario capacitar al personal de Tecnologías de la Información para que pueda asegurar que los miembros de otros departamentos cumplan con las pautas establecidas en la Norma ISO 27002:2022. Esto ayudará a garantizar que todos los empleados estén en línea con los controles necesarios para mitigar riesgos en los sistemas de información.

- Mantener el procedimiento de gestión de solicitudes de información y fortalecer las políticas y herramientas utilizadas para garantizar su eficacia y eficiencia.
- Continuar aplicando y mejorando el procedimiento de Gestión de Activos de COARSA que establece un proceso riguroso y detallado.
- Crear directrices basadas en las políticas físicas y tecnológicas establecidas por la Norma ISO 27002, dado que proporcionarían un marco claro y consistente para la implementación de estos controles en toda la organización.

Referencias bibliográficas

Referencias bibliográficas

Aguirre, P. del C.; Anaya, M. del P.; Laurencio, R. L.; Casco López, J. (2013). Investigación aplicada e interdisciplinariedad en las ciencias de la comunicación. *Prisma Social*, (11), 294-320. https://www.redalyc.org/pdf/3537/353744535009.pdf

Agustina, M. (2019). Seguridad Informática: La Protección de la Información en una Empresa Vitivinícola de Mendoza, 2019. Universidad Nacional de Cuyo. Facultad de Ciencias Económicas. https://bdigital.uncu.edu.ar/objetos_digitales/15749/sistimariaagustina.pdf

Alonso, C. (2022, 24 mayo). *¿Qué son las normas ISO?* GlobalSuite Solutions. https://www.globalsuitesolutions.com/es/que-son-normas-iso/#:%7E:text=Las%20normas%20ISO%20son%20un,de%20productos%20en%20la%20industria.

Bobadilla Vera, L. R. (2022). *Mercado laboral y su influencia en la inserción de las/os secretarias/os del cantón Vinces* (Bachelor's thesis, BABAHOYO: UTB, 2022). http://dspace.utb.edu.ec/handle/49000/12188

Cabrera Mercado, K. M., Barreto Gil, E. y Torres Archibold, J. (2021). *Desarrollo de página web y gestor de contenidos de la Institución Educativa Flowers Hill Bilingual School de San Andrés Islas* (Bachelor's thesis, Corporación

Universidad de la Costa). http://repositorio.unibe.edu.ec/handle/123456789/386

Capeta, F. (2022, 21 marzo). *¿Sabes cuáles son las mejoras de la nueva ISO/IEC 27002:2022?* Global Trust Association. https://globaltrustassociation.org/es/sabes-cuales-son-las-mejoras-de-la-nueva-iso-270022022/

Colmenares R., M. A. (2020). *Auditoría al control de acceso del sistema de información Proyectoinnpulsa-udea de la Interventoría de la Universidad de Antioquía bajo la norma ISO/IEC 27002*. Universidad Católica de Colombia. Bogotá D. C. (*specialization in audit.*). https://repository.ucatolica.edu.co/bitstream/10983/24851/7/Auditor%c3%ada%20al%20SI%20Interventor%c3%ada%20UdeA%202020.pdf

Corvo, H. S. (2021, 6 julio). *Política informática*. Lifeder. 2022. https://www.lifeder.com/politica-informatica/

Diéguez Rebolledo, M. (2022). *Enfoque Metodológico para la selección de controles de seguridad de la información*.

Espinoza Mina, M. A. (2015, 22 julio). Importancia de los modelos para el gobierno de la seguridad de la información en las empresas: una revisión sistemática de la literatura. *Espacios*, *40*(25). https://www.revistaespacios.com/a19v40n25/a19v40n25p05.pdf

Figueroa L., J. L. (2019). *Plan de seguridad informática basado en la Norma ISO 27002 y la gestión de la información para el departamento de TIC de la*

Uniandes Extensión Babahoyo. Universidad Regional Autónoma de los Andes. Babahoyo, Ecuador (*Bachelor's thesis*). https://dspace.uniandes.edu.ec/bitstream/123456789/9751/1/PIUBSIS001-2019.pdf

Fuentes C., J. M (mayo, 2019). *Auditoría al sistema de gestión de la información del proceso de gestión de incidentes de clientes de ANS Comunicaciones, con base en la norma técnica colombiana NTC-ISO/IEC 27002*. Universidad Católica de Colombia, Bogotá D.C (*specialization in audit.*). https://dspace.ups.edu.ec/handle/123456789/3163

Galeano, M. E. (2020). Diseño de proyectos en la investigación cualitativa. Universidad Eafit. https://books.google.es/books?id=Xkb78OSRMI8C&lpg=PA11&ots=zsJrgTPFuL&dq=Este%20enfoque%20cuantitativo%20trabaja%20sobre%20la%20base%20de%20una%20revisi%C3%B3n%20de%20literatura%20que%20apunta%20al%20tema%20y%20da%20como%20conclusi%C3%B3n%20un%20marco%20te%C3%B3rico%20orientador%20de%20la%20investigaci%C3%B3n&lr&hl=es&pg=PA11#v=onepage&q&f=false

Hernández García., D. (2019). *Diseño e implementación de un esquema de seguridad de nivel 0 a nivel1 basado en las normas ISO 27002: 2013*. Escuela Superior Politécnica del Litoral, Guayaquil, Ecuador (*Master´s tesis).* https://dspace.ups.edu.ec/handle/123456789/3163

International Organization for Standardization. (2022). *Information security and privacy protection – Information security controls (ISO 27002)* (3rd edition).

López, A. (s. f.). *Recursos*. ISO2700.ES. https://www.iso27000.es/iso27002.html

López, S. (Marketing Digital). (2019, 8 noviembre). *¿Qué es ISO?* SPG Certificación | Certificado ISO 9001. https://www.certificadoiso9001.com/que-es-iso/

Lovos Turcios, F. D. (setiembre, 2019). *Seguridad Física y Lógica en los Centros de Cómputo* [Diapositivas de PowerPoint]. Auditoría de Sistemas Computarizados. Universidad de Oriente. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiuy8X87s_5AhV9mIQIHQPfB4k4FBAWegQICBAB&url=https%3A%2F%2Flovosfrancisco.jimdofree.com%2Fapp%2Fdownload%2F9167889769%2FSEGURIDAD%2BFISICA%2BY%2BLOGICA.pdf%3Ft%3D1549054595&usg=AOvVaw1bw9UAWWs2EvWd1gBE3OoB

Mata D., M. S. (2019). *Marco metodológico de investigación*. Investigaliacr. https://investigaliacr.com/investigacion/marco-metodologico-de-investigacion/

Murillo P., D. C. (2021). *Políticas de Seguridad de la Información Basado en Normas ISO 27002 para el Departamento Informático de la Universidad Estatal del Sur de Manabí*. Universidad Estatal del Sur de Manabí. Jipijapa- Manabí-Ecuador.

Riesco, S. (2018, 9 noviembre). ¿Cuáles son las normas ISO más importantes? *Formazion*. https://www.formazion.com/noticias_formacion/cuales-son-las-normas-iso-mas-importantes-org-5273.html#:%7E:text=Una%20norma%20

ISO%20es%20un,experiencia%20y%20el%20desarrollo%20tecnol%C3%B3gico.

Rosh, C. (2022). Un ciberataque masivo en Costa Rica aflige a la ciudadanía. Reporting Global Tech Stories. https://restofworld.org/2022/ciberataque-costa-rica-ciudadania/#:~:text=Los%20ciberdelincuentes%20comenzaron%20atacando%20al,no%20negociar%C3%ADa%20con%20%E2%80%9C%20terroristas%E2%80%9D

Ruiz, J. J. (2019, 9 mayo). *La seguridad en tu negocio: Seguridad Lógica y Física. – Consultores y Soporte AMD*. Consultores y Soporte AMD. http://cysamd.com.mx/seguridad/seguridad-negocio-seguridad-logica-fisica/

Salazar Choez, T. K. (2018). Análisis de la norma ISO/IEC 27002: 2013 para mejorar los controles de la seguridad de la información en la sala de cómputo# 14 de la Carrera de Ingeniería en Computación y Redes (*Bachelor's thesis*, jipijapa-unesum) http://repositorio.unesum.edu.ec/handle/53000/1469

Salazar-Escorcia, L. S. (2020). Investigación Cualitativa: Una respuesta a las Investigaciones Sociales Educativas. *CIENCIAMATRIA*, *6*(11), 101-110. http://cienciamatriarevista.org.ve/index.php/cm/article/view/327

Sánchez Vela, M. A. (2021). *Elaboración de un Plan de Seguridad Informática para Mejorar la Gestión de la Información de la Sub-Gerencia de Tecnología de la Información, de la Municipalidad Provincial de Requena-2021*. Facultad de Ciencias e Ingeniería, San Juan Bautista, Maynas, Loreto, Perú (*Bachelor's*

thesis, jipijapa-unesum) http://repositorio.unesum.edu.ec/handle/53000/1469.

Sandoval F., L. R. (2019). *Modelo de buenas prácticas aplicando ISO 27002 para la gestión de incidencias de la red Wncor. Universidad Peruana Los Andes.* Lima, Perú (*Bachelor's thesis*). https://repositorio.upla.edu.pe/bitstream/handle/20.500.12848/1355/T037_73471588_T.pdf?sequence=1&isAllowed=y

Tovar O., E. F. (2022, 2 marzo). *Actualizaciones de la ISO 27002 y su Impacto*. LinkedIn. https://es.linkedin.com/pulse/actualizaciones-de-la-iso-27002-y-su-impacto-evans-f-tovar-o-

Universidad Autónoma del Estado de Hidalgo. (s. f.). *UAEH: Dirección de Educación Media Superior* ¿Qué es una lista de cotejo para evaluar tareas? https://www.uaeh.edu.mx/division_academica/educacion-media/

Universidad Latina de Costa Rica. (2020, 23 julio). *¿Cuáles son las 7 normas ISO más importantes del mundo y para qué sirven?* https://www.ulatina.ac.cr/articulos/cuales-son-las-7-normas-iso-mas-importantes-del-mundo-y-para-que-sirven#:~:text=La%20International%20Organization%20of%20Standardization,organizaci%C3%B3n*%20estableci%C3%B3%20para%20este%202018.

Vázquez Dominguez, B. D. (2019, mayo). *CRIM*. Centro Regional de Investigaciones Multidisciplinarias. https://www.crim.unam.mx/media/Politica-informatica-1.pdf

Vega Abad, C. R. (2018). Análisis y estudio de políticas de seguridad informática para un ISP con usuarios residenciales. Pro Sciences: *Revista de Producción, Ciencias e Investigación*, 2(8), 32–38. https://doi.org/10.29018/issn.2588-1000vol2iss8.2018pp32-38

Anexos

Anexos

Anexo 1: Manual de procedimentos operativos de análisis

MANUAL DE PROCEDIMIENTOS OPERATIVOS DE ANÁLISIS Y ESTADÍSTICA

DPTO. INFORMÁTICA

Código: 07.1-MP-01

Versión 1.0

San Ramón, Costa Rica

Mayo, 2021

LISTA DE RESPONSABLES SEGÚN ROL

Rol	Nombre/Cargo/Dependencia	Firma
Elaboró	Maripaz Araya Carvajal	X Maripaz Araya Carvajal Estudiante
Revisó	Ing. Kirk Solórzano Almendarez. *Departamento de Tecnología Informática*	X Kirk Solorzano Almendarez IT Manager
Aprobó	Lic. Kattya Alpízar Quesada. *Gerente administrativa*	X Lic. Kattya Alpízar Gerente Administrativo
Validó	Mba. Leonardo Arguedas Cruz. *Gerente general*	X Mba. Leonardo Arguedas Gerente General

	Lic. Kattya Alpízar Quesada. *Gerente administrativa*	X Lic. Kattya Alpízar Gerente Administrativo

CONTENIDO

SIGLAS, ABREVIATURAS Y CONCEPTOS

CONCEPTOS

WETRANSFER: Aplicación basada en la transferencia de archivos especialmente pesados, por medio de la nube.

DROPBOX: Herramienta que permite sincronizar archivos a través de un directorio virtual o disco duro virtual de la red.

GOOGLE DRIVE: Servicio de alojamiento de archivos.

FTP: File Transfer Protocol o FTP, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red.

NARRATIVA DEL PROCEDIMIENTO

00- Inicio del procedimiento

01- El encargado recibe una solicitud de información por parte de los colaboradores de la empresa o proveedores y colaboradores de los proveedores.

02- Toma de Requerimientos. El encargado realiza una toma de requerimientos al usuario por un medio de correo electrónico, WhatsApp o llamada.

Nota: los requerimientos deben especificar parámetros, objetivos y necesidades.

Nota: en caso de que el usuario se comunique vía telefónica, debe asimismo, dejar por escrito el requerimiento solicitado, ya sea al WhatsApp de Soporte Técnico o vía correo electrónico.

03- El encargado debe tener una autorización previa de su jefe inmediato para proceder con la solicitud del usuario.

Nota: toda información solicitada por un colaborador de su propia área puede brindarse sin autorización previa.

Nota: Política TI-PO-07 (Seguridad de la Información- Apartado 9.)

04- El encargado analiza la solicitud y define si es un documento ya existente o si se debe desarrollar.

05- ¿Se trata de un documento existente?

Nota: Si el documento ya es existente, se debe dirigir al punto 10.

Si el documento no es existente, se debe desarrollar se continua en el punto 06.

06- El encargado realiza un análisis de los requerimientos del usuario

07- El encargado realiza una retroalimentación al usuario con posibles soluciones, viabilidad y tiempo de respuesta.

08- El encargado desarrolla los requerimientos del usuario por medio de herramientas informáticas

Nota: las herramientas informáticas utilizadas son: herramientas de programación, herramientas de bases de datos, reporteadores, Excel. Herramientas para compartir información son únicamente las herramientas autorizadas por la empresa y los socios comerciales.

Nota: Política TI-PO-07 (apartado 9.1 punto g)

09- El encargado le presenta al usuario lo desarrollado y le realiza la debida entrega.

10- El usuario realiza un acuse de satisfecho.

Nota: si el usuario necesita modificar el producto final, debe enviar una solicitud con las modificaciones necesarias para volver a iniciar el procedimiento anteriormente detallado.

11- Fin del procedimiento.

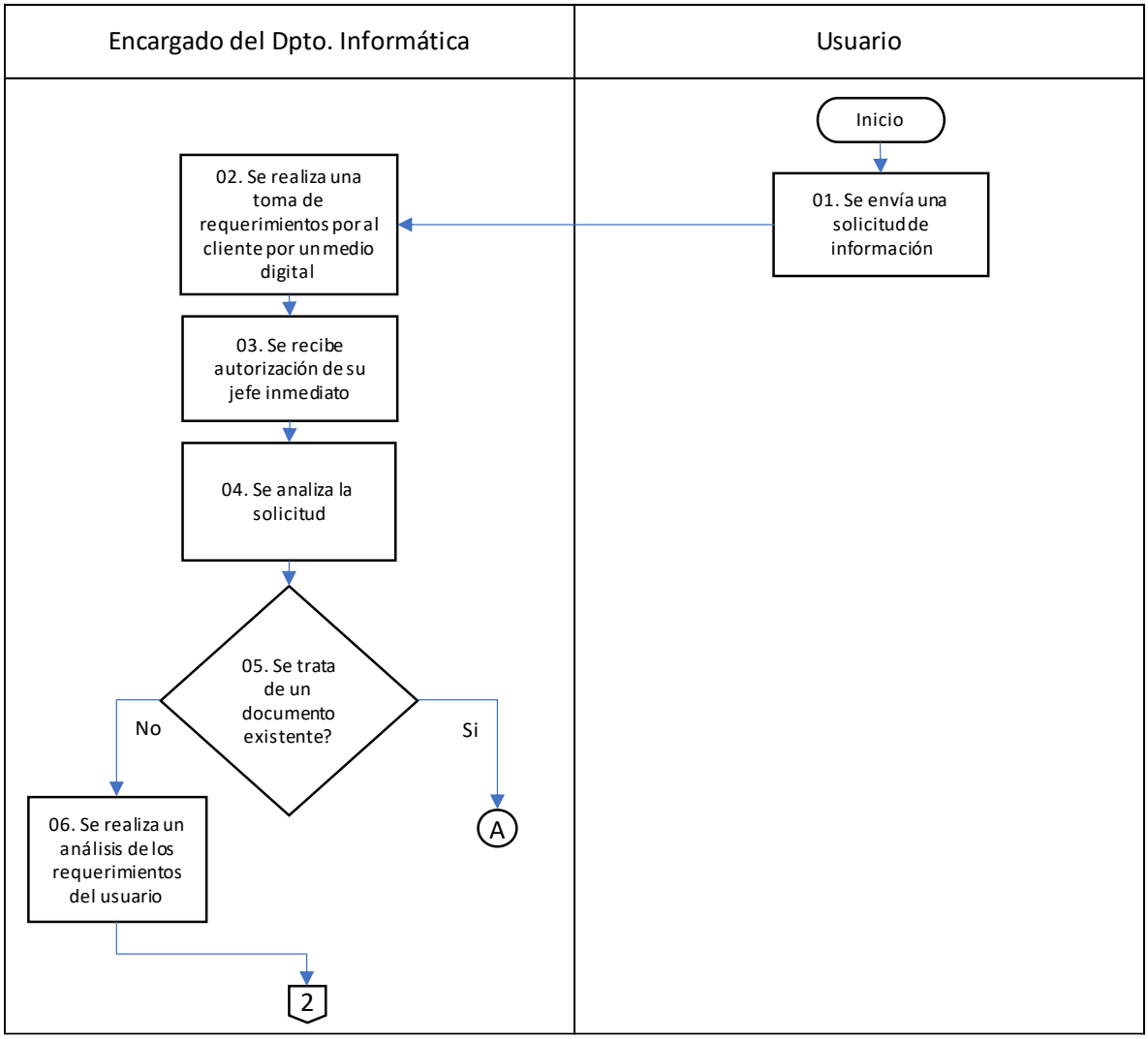
FICHA TÉCNICA

Ficha Técnica	
	**Nombre del Procedimiento:** Análisis de Datos y Estadística
	Objetivo: llevar a cabo una correcta gestión de las solicitudes de información por parte del usuario, tanto en el desarrollo de las solicitudes como en la entrega final de la documentación.
Alcance	**Empieza:** el procedimiento inicia cuando el encargado recibe una solicitud de información por parte de los colaboradores de la empresa o proveedores y colaboradores de los proveedores.
	Incluye: se debe llevar a cabo funciones como recepción de solicitudes de usuarios, uso de diferentes sistemas informáticos (Excel, herramientas de programación, herramientas de bases de datos, reporteadores, Excel. herramientas para compartir información como Wetransfer, Dropbox, Google drive, FTP, carpetas compartidas dentro de la organización.)
	Termina: el procedimiento finaliza cuando el usuario envía un acuse de satisfecho.
Requerimientos	**Entradas:** documentación para la solicitud de información.

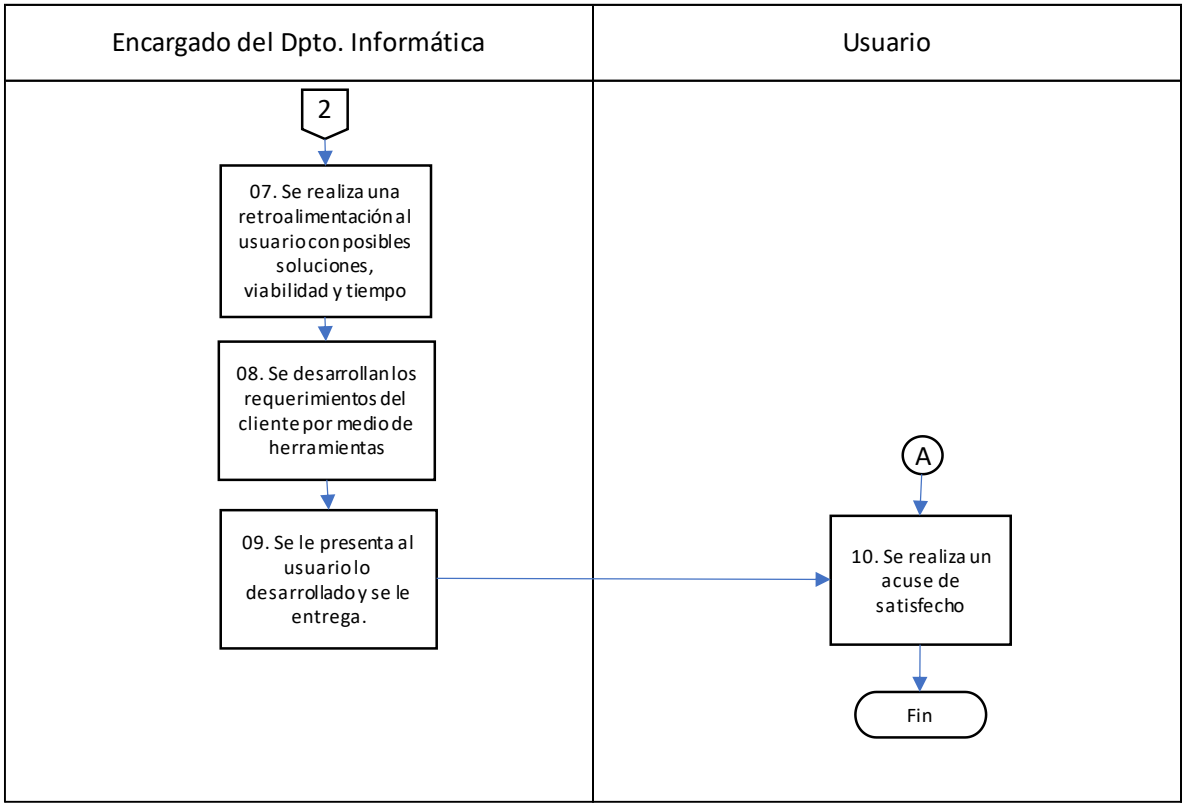
	Proveedores: usuarios internos de la compañía, proveedores, documentos de autorización.
	Salidas: documentación solicitada por el usuario
	Usuarios: usuarios internos de la compañía y proveedores

DIAGRAMA DE ACTIVIDADES

DISTRIBUIDORA coarsa DISTRIBUCION Y COBERTURA DE CALIDAD	Coarsa S. A- Dpto. Informática	Versión: 0.1
		Código : DCT-07.0-P01
	Procedimiento de Análisis de Datos y Estadistica	Página: 1 de 2



DISTRIBUIDORA coarsa DISTRIBUCIÓN Y COBERTURA DE CALIDAD	Coarsa S. A- Dpto. Informática	Versión: 0.1
		Código : DCT-07.0-P01
	Procedimiento de Análisis de Datos y Estadistica	Página: 1 de 2



Anexo 2: Manual de procedimientos operativos de gestión de activos

MANUAL DE PROCEDIMIENTOS OPERATIVOS DE GESTIÓN DE ACTIVOS

DPTO. INFORMÁTICA

Código: 07.2-MP-01

Versión 1.0

San Ramón, Costa Rica

Junio, 2021

CONTENIDO

LISTA DE RESPONSABLES SEGÚN ROL

Rol	Nombre/Cargo/Dependencia	Firma
Elaboró	Maripaz Araya Carvajal	X Maripaz Araya Carvajal Estudiante
Revisó	Kirk Solórzano Almendarez *TI*	X Kirk Solorzano Almendarez IT Manager
Aprobó	Lic. Kattya Alpízar Quesada. *Gerente administrativa*	X Lic. Kattya Alpízar Gerente Administrativo
Validó	Mba. Leonardo Arguedas Cruz. *Gerente general*	X Msc. Leonardo Arguedas Gerente General

	Lic. Kattya Alpízar Quesada. *Gerente administrativa*	X Lic. Kattya Alpízar Gerente Administrativo

SIGLAS, ABREVIATURAS Y CONCEPTOS

CONCEPTOS

ACTIVO: conjunto de bienes o recursos de los que es propietaria la compañía.

***CHECKLIST*:** se trata de un ahoja de verificación o lista de requisitos. Su uso en este procedimiento será especificar los componentes con los que se entrega el activo (cargador, estuche, vidrio temperado, audífonos) el estado en el que se encuentra (si posee algún golpe o alguna ruptura).

HOJA DE RECEPCIÓN DE ACTIVOS: Se trata de una hoja para mantener un adecuado registro con la persona responsable del activo, identificación, manejo y eficiente control de todos ellos. Su uso en este procedimiento será para que contenga una narrativa que el vendedor debe firmar, con la cual se hace responsable de los activos que la empresa la entrega, se debe anotar el nombre del

vendedor, número de cédula, además, se debe incluir el modelo del activo entregado y el número de serie.

NARRATIVA DEL PROCEDIMIENTO

00- Inicio del procedimiento.

01- Recursos Humanos informa sobre cualquier acción de personal que involucre la gestión de activos, al Departamento de Informática y al jefe inmediato del colaborador.

02- Jefe inmediato agenda una cita con el colaborador y el encargado(a) del Dpto. de Informática.

03- Encargado(a) del Dpto. de Informática alista los documentos que debe entregarle al colaborador.

Nota: al colaborador se le debe hacer entrega de una hoja de recepción de activos.

Nota: se realiza un *checklist*. Debe quedar en un repositorio del Departamento de Informática y una copia al responsable.

04- Colaborador se presenta a la empresa a realizar la gestión respectiva.

05- Encargado(a) del Dpto. de Informática hace entrega la hoja de entrega de activos y la hoja de *checklist*.

06- Colaborador responsable firma la hoja de *checklist* y el documento de entrega de activos, haciéndose responsable de los artículos que se le está entregando.

07- Encargado(a) del Dpto. de Informática firma la hoja de *checklist* y la hoja de entrega de activos anteriormente firmada por el responsable.

08- Encargado(a) del Dpto. de Informática hace entrega de los activos al responsable.

09- Encargado de Recursos Humanos informa al encargado(a) de otra acción de personal para dicho colaborador que involucra la gestión de activos.

10- Jefe inmediato agenda una cita con el colaborador y el encargado(a) del Dpto. de Informática.

11- Encargado(a) del Departamento de Informática imprime los documentos de control que tiene almacenados en la computadora, necesarios para el día de la visita.

Nota: los documentos necesarios son la hoja de *check list* y documento de recepción de activos

12- Colaborador se presenta a la empresa, según la cita previa anteriormente definida entre su jefe inmediato y el encargado(a) del Departamento de Informática para hacer entrega de los activos y llevar a cabo la firma de los documentos establecidos.

13- Colaborador hace entrega de los activos al encargado(a) del Departamento de Informática.

14- Encargado(a) del Departamento de Informática revisa los activos entregados contra el *check list* que se realizó en el momento de la entrega del activo.

15- ¿Se encuentra todo en orden?

a 1. Si se devuelve todo en orden se avanza al punto 21

a 2. De lo contario, se cotiza, ya sea la reparación o el artículo faltante y se continua en el punto 16.

16- Encargado(a) del Departamento de Informática le informa al jefe inmediato sobre el daño del artículo o el faltante de activos.

17- Encargado(a) del Departamento de Informática envía un reporte sobre lo sucedido a Recursos Humanos, junto con una cotización, ya sea por la reparación de los daños, compra de artículos faltantes o remplazo del activo dañado.
18- Recursos Humanos determina de qué manera se debe proceder.
19- Encargado(a) del Departamento de Informática actualiza el archivo digital registrando los cambios generados en torno al estado de los activos y su asignación.
20- Encargado(a) del Departamento de Informática almacena los activos en su lugar respectivo.
21- Encargado(a) del Departamento de Informática hace entrega de los documentos previamente firmados al encargado(a) de Recursos Humanos.
22- Fin del procedimiento.

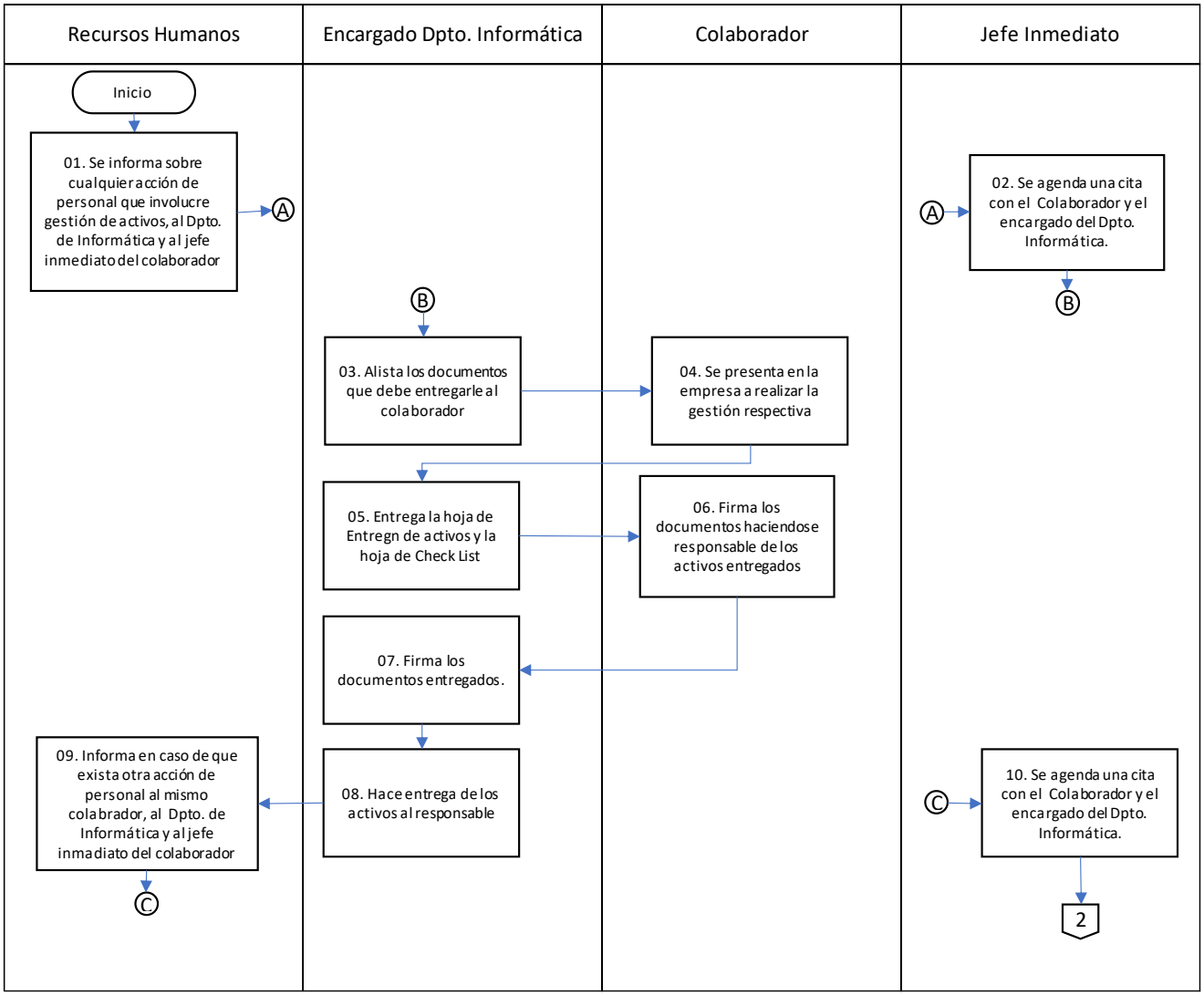
FICHA TÉCNICA

<table>
<tr><th colspan="3">Ficha Técnica</th></tr>
<tr><td rowspan="3">  </td><td rowspan="2">COARSA S. A. - Dpto. Informática</td><td>Versión: 0.1</td></tr>
<tr><td>Código: DCT-0.07-P01</td></tr>
<tr><td>Procedimiento de Gestión de Activos</td><td>Página: 1 de 1</td></tr>
<tr><td colspan="2">Objetivo: llevar a cabo una correcta gestión de la entrega de activos propiedad de COARSA a los vendedores.</td></tr>
<tr><td rowspan="3">Alcance</td><td colspan="2">Empieza: el procedimiento inicia cuando el encargado(a) de Recursos Humanos informa sobre cualquier acción de personal que involucre la gestión de activos al encargado(a) del Dpto. de Informática y al jefe inmediato del colaborador.</td></tr>
<tr><td colspan="2">Incluye: se deben llevar a cabo funciones como, comunicación fluida entre Recursos Humanos y el supervisor(a) encargado(a) de los vendedores, chequeo de activos, manejo de documentos y registros sobre los activos.</td></tr>
<tr><td colspan="2">Termina: el procedimiento finaliza cuando el encargado(a) del Dpto. de Informática hace entrega de los documentos firmados al encargado(a) de Recursos Humanos.</td></tr>
<tr><td rowspan="2">Requerimientos</td><td colspan="2">Entradas: acciones de personal.</td></tr>
<tr><td colspan="2"></td></tr>
</table>

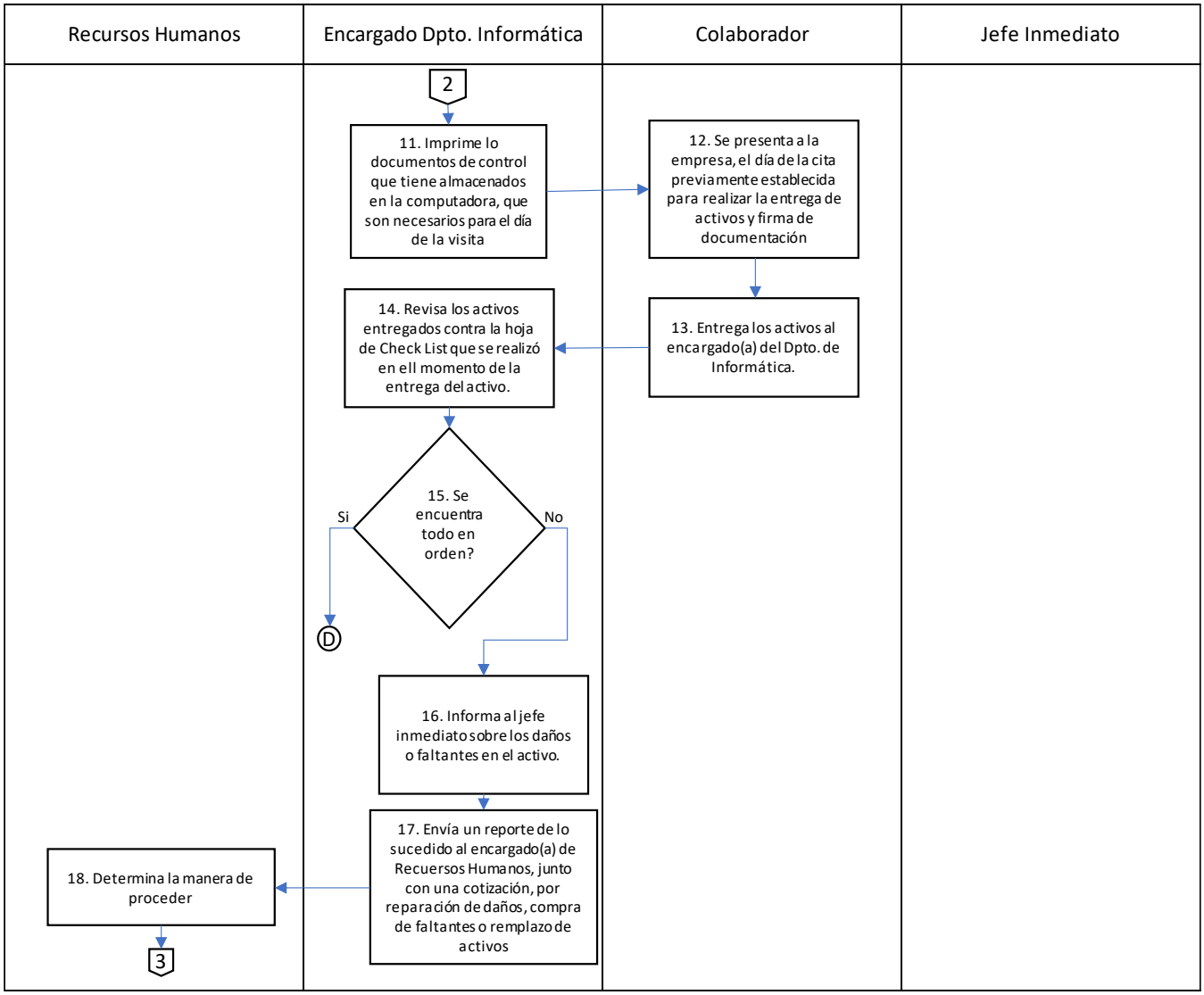
	Proveedores: Recursos Humanos
	Salidas: activos entregados y/o recibidos de colaboradores para su uso responsable.
	Usuarios: colaboradores

DIAGRAMA DE ACTIVIDADES

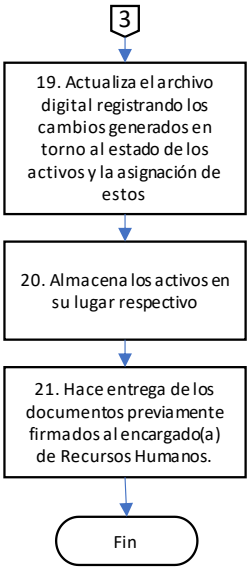
Distribuidora coarsa distribución y cobertura de calidad	Coarsa S. A- Dpto. Informática	Versión: 0.1
		Código : DCT-0.07-P01
	Procedimiento de Entrega de Activos	Página: 1 de 3



Distribuidora coarsa	Coarsa S. A- Dpto. Informática	Versión: 0.1
		Código : DCT-0.07-P01
	Procedimiento de Entrega de Activos	Página: 2 de 3



Distribuidora coarsa distribución y cobertura de calidad	Coarsa S. A- Dpto. Informática	Versión: 0.1
		Código : DCT-0.07-P01
	Procedimiento de Entrega de Activos	Página: 3 de 3

Recursos Humanos	Encargado Dpto. Informática	Colaborador	Jefe Inmediato
			

Anexo 3: Manual de procedimientos operativos de soporte técnico

MANUAL DE PROCEDIMIENTOS OPERATIVOS DE SOPORTE TÉCNICO

DPTO. DE INFORMÁTICA

Código: 07.0-MP-01

Versión 1.0

San Ramón, Costa Rica

Julio, 2021

LISTA DE RESPONSABLES POR ROL

Rol	Nombre/Cargo/Dependencia	Firma
Elaboró	Maripaz Araya Carvajal	X Maripaz Araya Carvajal Gestor de Procesos
Revisó	Ing. Kirk Solórzano Almendraez. *Departamento de Tecnología Informática*	X Kirk Solorzano Almendarez IT Manager
Aprobó	Lic. Kattya Alpízar Quesada. *Gerente administrativa*	X Lic. Kattya Alpízar Gerente Administrativo

Validó	Mba. Leonardo Arguedas Cruz. *Gerente general*	X Mba. Leonardo Arguedas Gerente General
	Lic. Kattya Alpízar Quesada. *Gerente administrativa*	X Lic. Kattya Alpízar Gerente Administrativo

CONTENIDO

SIGLAS, ABREVIATURAS Y CONCEPTOS

CONCEPTOS

ANYDESK: es un programa de software de escritorio remoto, provee acceso remoto bidireccional entre computadoras personales.

TEAMVIEWER: es un software informático “privado” de fácil acceso, que permite conectarse remotamente a otro equipo. Entre sus funciones están: compartir y controlar escritorios, reuniones en línea, videoconferencias y transferencia de archivos entre ordenadores.

PROVEEDOR DE SERVICIO: persona o empresa que presta servicios a la empresa.

PROVEEDOR DE INSUMOS: persona o empresa que abastece de insumos u otros suministros a la empresa.

ACTIVO: un activo es un bien que la empresa posee, equivalente a un valor mayor o igual a ₡106 000.

GASTO: es la utilización o consumo de un bien o servicio a cambio de una contraprestación, se suele realizar mediante una cantidad saliente de dinero.

PUESTOS INVOLUCRADOS

- **Jefe del departamento**
- **Colaborador del departamento**

En el procedimiento de soporte técnico ambos puestos tienen inherencia y ambos brindan soporte y atienen las solicitudes de los usuarios.

NARRATIVA DEL PROCEDIMIENTO

SOPORTE TÉCNICO

00-Inicio del procedimiento.

01-El usuario realiza una llamada o redacta un mensaje por medio del correo electrónico o los grupos de WhatsApp de Soporte Técnico correspondientes, solicitando soporte de TI, consultas respecto a TI y solicitudes de algún equipo informático.

Nota: si el usuario solicita soporte técnico, consultas o la solicitud de equipo informático por medio de una llamada telefónica también debe realizar la solicitud por algún medio escrito, ya sea correo electrónico o al WhatsApp de Soporte Técnico, a fin de quede evidenciado.

02-¿Se trata de un caso de Soporte Técnico / Consulta?

a 1. Si se trata de un caso de soporte técnico / consulta se debe continuar en el punto 09.

a 2. Si por lo contrario, se trata de solicitud de artículos informáticos debe continuar en el punto 03.

03-El encargado(a) del Dpto. de Informática primeramente debe valorar el requerimiento técnico y viabilidad para la empresa, posteriormente chequear si se cuenta con el artículo en el inventario.

04-¿Se cuenta con el artículo?

a 1. Si se cuenta con el artículo, se realiza la entrega del artículo y se completan los formularios correspondientes.

a 2. Si no se cuenta con el artículo, se procede a realizar la gestión para la adquirir el articulo con el proveedor de insumos y se procede con el punto 05.

05- El encargado(a) del Dpto. de informática coordina la logística para hacer llegar el artículo hasta la empresa, con el encargado de Bodega.

06- Proveedor envía la factura electrónica al encargado(a) del Dpto. de Contabilidad y este define si se trata de un activo o de un gasto.

07- ¿Se trata de un Activo?

Notas:

a 1. Si se trata de un activo, se debe ingresar el activo, bajo el manual ***07.2-MP-01 Gestión de Activos*** y posteriormente se continua con el punto 08.

a 2. Si por el contrario se trata de un gasto, se continua con el punto 08.

08- El encargado(a) del Dpto. de Informática hace entrega del artículo al usuario.

Nota: continua en el punto 18.

09- El encargado del Dpto. de Informática, si se trata de soporte técnico, realiza un diagnóstico del problema solicitado y decide si el problema se puede resolver por los encargados de TI o se necesita acudir a un proveedor de servicios.

Nota: encargado(a) del Dpto. de Informática, tiene un tiempo de respuesta de 0 a 3 horas, para enviar el diagnóstico o la respuesta al caso, al usuario.

10- ¿Se puede resolver por los encargados de TI?

Notas:

a 1. Si se puede resolver por el equipo de TI, se continua en el punto 11.

a 2. Si no se puede, se debe contactar al proveedor en caso de que la solución dependa de terceros y se continua en el punto 15.

11- El encargado agenda una cita con el usuario para proporcionar el soporte.

Nota: la prioridad de atención del caso la establece Gerencia, de acuerdo con el impacto que pueda tener en los diferentes procesos del negocio.

12- El encargado brinda soporte por medio de correo electrónico, WhatsApp, llamada telefónica, de forma remota (AnyDesk, TeamViewer) o de forma presencial.

Nota: para ingresar de manera presencial (en la estación de trabajo) y remota, ya sea por AnyDesk o TeamViewer, se debe tener autorización previa del responsable del equipo y el usuario debe de estar presente en el momento en el que se brinda el soporte hasta que concluya, lo cual se le recordará al usuario. En caso de que el inconveniente no tenga solución inmediata, se retomara el caso cuando exista una solución definitiva, aplicando la condición de presencialidad en las consecuentes visitas para la ejecución de la solución definitiva.

13- ¿Encargado le da solución al problema?

Notas:

a 1. Si el encargado le da solución al problema se continua en el punto 18

a 2. Si el encargado no le da solución al problema debe continuar en el punto 14.

14- El encargado se contacta con el proveedor para realizar la gestión del caso.

15- Encargado del Departamento de Informática realiza la gestión de la solución con el proveedor servicios.

Nota: el tiempo de respuesta después de realizar la gestión con el proveedor está sujeta solamente a la disponibilidad del proveedor.

16- El encargado mantiene comunicación activa con el proveedor hasta que finalice la gestión.

17- El proveedor realiza una retroalimentación al encargado(a) del Departamento de Informática sobre el caso.

18- El encargado brinda retroalimentación al usuario sobre el caso, o la compra, por algún medio escrito, ya sea correo o WhatsApp.

19- Fin del procedimiento.

FICHA TÉCNICA

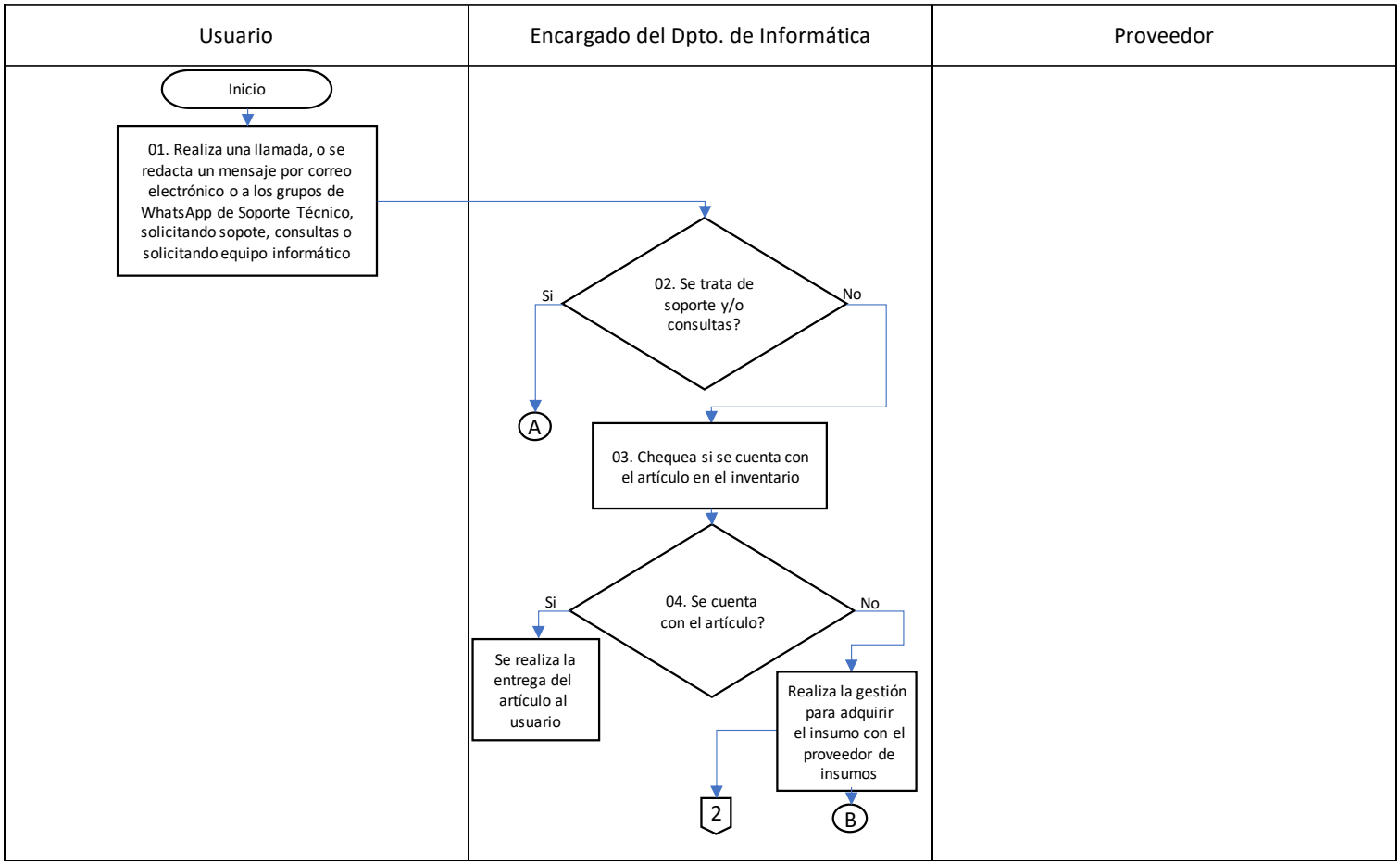
Ficha Técnica	
Distribuidora coarsa distribución y cobertura de calidad	**Nombre del Procedimiento:** Soporte Técnico
	Objetivo: llevar a cabo un correcto gestionamiento de los casos de soporte técnico, tanto la respuesta al cliente como la resolución de problemas y consultas por parte del usuario.
Alcance	**Empieza:** el procedimiento empieza cuando el encargado recibe un mensaje por correo o mediante WhatsApp del cliente, solicitando soporte técnico de TI, consultas respecto a TI o solicitudes de algún equipo informático.
	Incluye: Mantenimiento interno, mantenimiento predictivo, atención a usuarios, compra de insumos, comunicación con proveedores de insumos o proveedores de servicios.

	Termina: el procedimiento finaliza cuando se brinda retroalimentación al usuario sobre el caso o la compra, por algún medio escrito, ya sea correo o WhatsApp.
Requerimientos	**Entradas:** reporte de casos al Departamento de Informática por parte de los usuarios.
	Proveedores: contratista en servicios de software, contratista en servicios de impresión, contratista en CCTV, servicios técnicos en reparación de computadoras, proveedor de equipo informático.
	Salidas: resolución del caso reportado, consultas realizadas o compra de artículos.
	Usuarios: colaboradores internos de la empresa y proveedores.

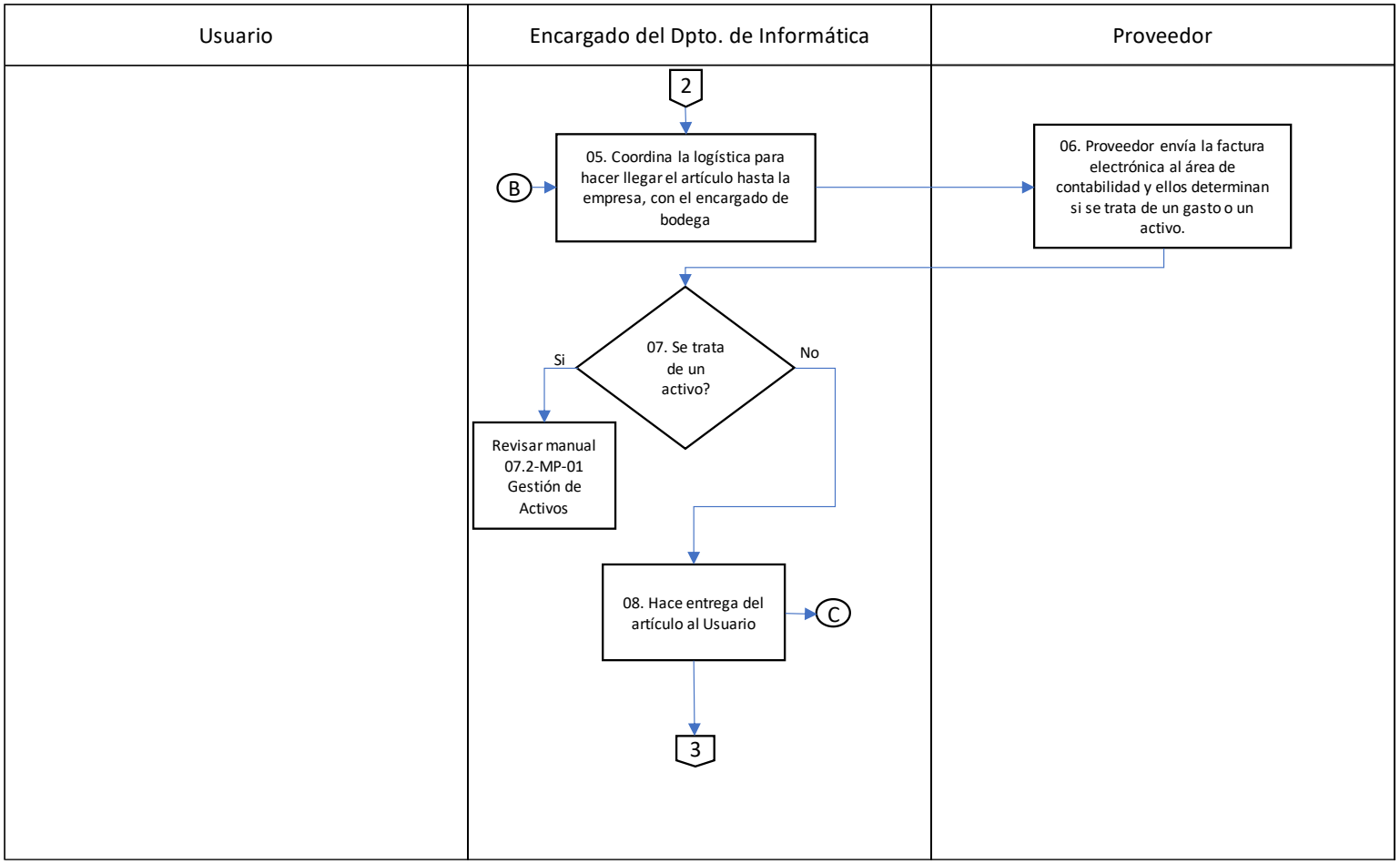
DIAGRAMA DE ACTIVIDADES

SOPORTE TÉCNICO

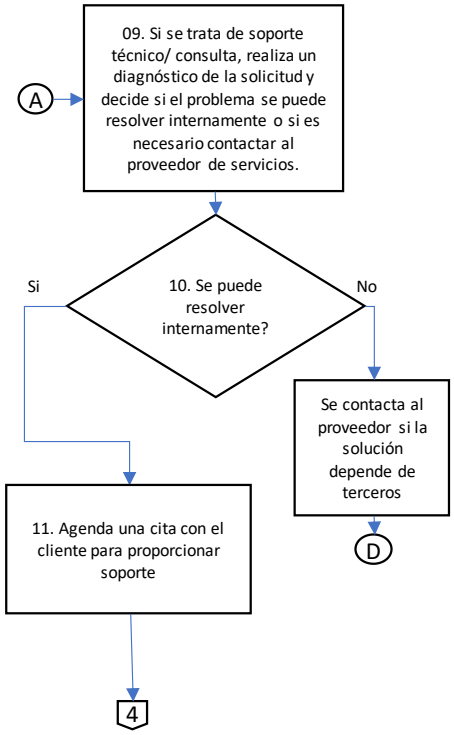
Distribuidora coarsa	Coarsa S. A- Dpto. Informática	Versión: 0.1
		Código : DCT-07.0-P01
	Procedimiento de Soporte Técnico	Página: 1 de 5



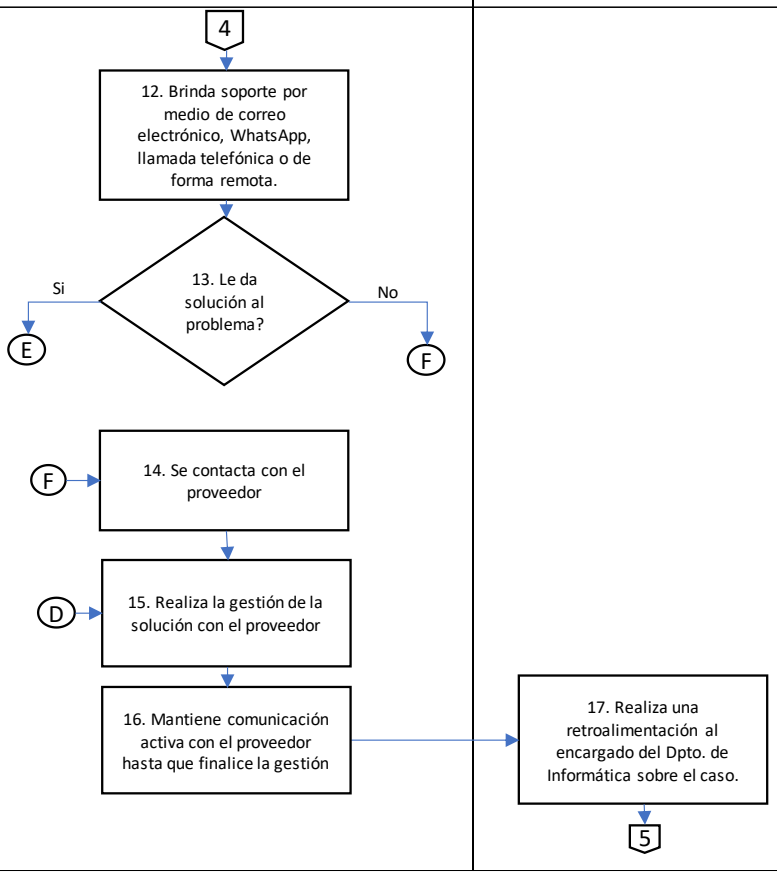
Distribuidora coarsa	Coarsa S. A- Dpto. Informática	Versión: 0.1
		Código : DCT-07.0-P01
	Procedimiento de Soporte Técnico	Página: 2 de 5



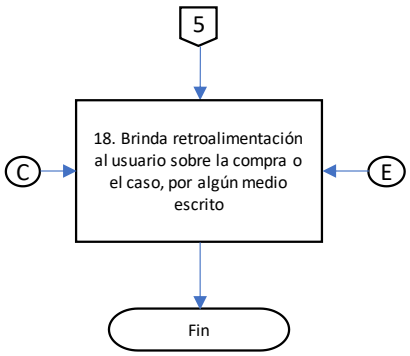
Distribuidora coarsa	Coarsa S. A- Dpto. Informática	Versión: 0.1
		Código : DCT-07.0-P01
	Procedimiento de Soporte Técnico	Página: 3 de 5

Usuario	Encargado del Dpto. de Informática	Proveedor
		

Distribuidora coarsa	Coarsa S. A- Dpto. Informática	Versión: 0.1
		Código : DCT-07.0-P01
	Procedimiento de Soporte Técnico	Página: 4 de 5

Usuario	Encargado del Dpto. de Informática	Proveedor
		

Distribuidora coarsa	Coarsa S. A- Dpto. Informática	Versión: 0.1
		Código : DCT-07.0-P01
	Procedimiento de Soporte Técnico	Página: 5 de 5

Usuario	Encargado del Dpto. de Informática	Proveedor
		

Anexo 4: Encuesta

UNIVERSIDAD TÉCNICA NACIONAL, SEDE DEL PACÍFICO

LICENCIATURA EN INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN

ANALIZAR LOS CONTROLES PARA LA SEGURIDAD DE LA INFORMACIÓN IMPLEMENTADOS POR LA EMPRESA DISTRIBUIDORA COARSA, EN SAN RAMÓN DE ALAJUELA, DE ACUERDO CON LA NORMA ISO 27002, DURANTE EL SEGUNDO SEMESTRE DEL AÑO 2022

FÓRMULA DE CONSENTIMIENTO INFORMADO

Encuesta para identificar como el personal de la empresa Distribuidora COARSA implementa los controles físicos y tecnológicos durante su jornada laboral

Estimados (as) señores(as):

Esta encuesta tiene como finalidad recopilar la información necesaria para elaborar un proyecto de graduación sobre los controles para la seguridad de la información implementados por la empresa Distribuidora COARSA, en San Ramón de Alajuela, de acuerdo con la Norma ISO 27002:2022, durante el segundo semestre del año 2022.

Se solicita su colaboración para contestar algunas preguntas, referentes a los controles para la seguridad de la información, implementados por la empresa.

Cabe destacar que las respuestas que nos brinde son estrictamente confidenciales y se utilizarán únicamente para efectos de este proyecto.

Si requiere más información puede comunicarse con nosotros(as), William García Molina, cédula 6-0436-0917 y Michelle Rodríguez Hernández, cédula 6-0455-0898, estudiantes activos de la Universidad Técnica Nacional (UTN), Teléfonos: 8486-9786 /8721-2517 y a los correos electrónicos: wsgarciamo@est.utn.ac.cr / merodriguezher@est.utn.ac.cr

Yo_____, portador del número de cédula de identidad _____, luego de leer y comprender todos los detalles de esta investigación _____, estoy de acuerdo con mi participación en el proyecto.

Firma_____

Cédula_____

Yo _____, número de cédula_____, como testigo de la firma de este contrato de consentimiento, afirmo que leí y comprendí el documento en su totalidad.

Firma_____

UNIVERSIDAD TÉCNICA NACIONAL

LICENCIATURA EN INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN

ANALIZAR LOS CONTROLES PARA LA SEGURIDAD DE LA INFORMACIÓN IMPLEMENTADOS POR LA EMPRESA DISTRIBUIDORA COARSA, EN SAN RAMÓN DE ALAJUELA, DE ACUERDO CON LA NORMA ISO 27002, DURANTE EL SEGUNDO SEMESTRE DEL AÑO 2022

INSTRUMENTO DE RECOLECCIÓN DE INFORMACIÓN

Encuesta para identificar como el personal de la empresa Distribuidora COARSA implementa los controles físicos y tecnológicos durante su jornada laboral

Estimados funcionarios(as):

Somos estudiantes de la Universidad Técnica Nacional y como parte de nuestro proyecto final de graduación, estamos realizando una encuesta que tiene como objetivo recolectar la información necesaria para identificar cómo el personal de la empresa Distribuidora COARSA, implementa los controles físicos y tecnológicos durante su jornada laboral. Cabe destacar que las respuestas que nos brinden son estrictamente confidenciales y se utilizarán únicamente para efectos de este proyecto.

A continuación, se les presenta una serie de preguntas relacionadas con dichos controles, las cuales están basadas en la Norma ISO 27002:2022.

A. Información general

¿Cuántos años tiene de laborar en la empresa?

( ) 1-5 años

( ) 6-10 años

( ) Más de 10 años

B. Controles físicos y tecnológicos

1. **Cuando necesita acceder a una zona restringida, ¿se le solicita alguno de los siguientes mecanismos técnicos para la gestión del acceso?**

   ( ) Tarjeta o gafete de acceso

   ( ) Biometría (huella digital, reconocimiento facial etc.)

   ( ) Autenticación de dos factores

   ( ) PIN secreto

   ( ) Ninguno de los anteriores

2. **En los casos en los que requiere acceder a información confidencial de la empresa, ¿debe firmar o registrarse en algún libro físico o electrónico?**

   ( ) Sí

   ( ) No

   ( ) No aplica para mi cargo

3. **Al ingresar o salir de las instalaciones de la empresa, ¿el personal de seguridad inspecciona sus pertenencias?**

    ( ) Únicamente al ingresar

    ( ) Únicamente al salir

    ( ) En ambos casos

    ( ) No las inspeccionan

4. **¿Tiene permitido el uso de equipos fotográficos, de video, de audio u otro tipo de equipos de grabación durante su jornada laboral?**

    ( ) Sí

    ( ) No

5. **Al abandonar su área de trabajo por alguna u otra razón, ¿bloquea los dispositivos electrónicos como computadoras o tabletas con algún tipo de contraseña o mecanismo de bloqueo?**

    ( ) Sí

    ( ) No

    ( ) No aplica para mi cargo

6. **Si durante su jornada laboral requirió escribir información sensible o critica en pizarras o alguna otra parte de la oficina, ¿se asegura de eliminarla antes de retirarse de las instalaciones de la empresa?**

    ( ) Sí

    ( ) No

    ( ) No aplica para mi cargo

7. **¿La empresa tiene establecidas reglas para comer, beber y fumar en la cercanía de las instalaciones donde se realiza procesamiento de información?**

   ( ) Sí

   ( ) No

8. **¿La empresa cuenta con alguna política o reglas para el uso de servicios y aplicaciones en Internet?**

   ( ) Sí

   ( ) No

9. **¿Al imprimir algún tipo de información debe seguir ciertas reglas establecidas por la empresa?**

   ( ) Sí

   ( ) No

10. **¿La empresa tiene establecidas reglas y orientación para la configuración de ventanas emergentes en las pantallas (ejemplo, desactivar las nuevas ventanas emergentes de correo electrónico y mensajería, si es posible, durante presentaciones, pantallas compartidas o en un área pública)?**

    ( ) Sí

    ( ) No

    ( ) No aplica para mi cargo

11. **¿Alguna vez ha recibido algún tipo de capacitación sobre cómo identificar y mitigar de forma potencial la recepción, envió o instalación de correos electrónicos, archivos o programas infectados?**

    ( ) Sí

    ( ) No

12. **¿Conoce si la organización cuenta con controles para minimizar el riesgo de posibles amenazas físicas y ambientales, por ejemplo, robo, incendio, explosivos, humo, agua etc.?**

    ( ) Sí

    ( ) No

13. **Cuando necesita retirar equipos y medios de las instalaciones de la organización, ¿se le solicita algún tipo de autorización?**

    ( ) Sí

    ( ) No

    ( ) No aplica para mi cargo

14. **Si por alguna razón requiere retirar un equipo o medio de almacenamiento de las instalaciones, ¿se asegura de que este no quede desatendido o sin seguridad en público?**

    ( ) Sí

    ( ) No

    ( ) No aplica para mi cargo

15. **La computadora que utiliza para laborar ¿le permite el uso de dispositivos de almacenamiento extraíbles tales como llaves mayas, discos duros externos, tarjetas SD o algún otro medio de almacenamiento?**

    ( ) Sí

    ( ) No

    ( ) No aplica para mi cargo

Anexo 5: Lista de cotejo de controles físicos

UNIVERSIDAD TÉCNICA NACIONAL, SEDE DEL PACÍFICO

LICENCIATURA EN INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN

ANALIZAR LOS CONTROLES PARA LA SEGURIDAD DE LA INFORMACIÓN IMPLEMENTADOS POR LA EMPRESA DISTRIBUIDORA COARSA, EN SAN RAMÓN DE ALAJUELA, DE ACUERDO CON LA NORMA ISO 27002, DURANTE EL SEGUNDO SEMESTRE DEL AÑO 2022

FÓRMULA DE CONSENTIMIENTO INFORMADO

Lista de cotejo para verificar el cumplimiento de los controles físicos de la Norma ISO 27002:2022 por parte de la empresa Distribuidora COARSA

Estimados (as) señores(as):

Esta lista de cotejo tiene como finalidad recopilar la información para elaborar un proyecto de graduación sobre los controles para la seguridad de la información implementados por la empresa Distribuidora COARSA, en San Ramón de Alajuela, de acuerdo con la Norma ISO 27002:2022, durante el segundo semestre del año 2022.

Se solicita su colaboración para contestar algunos indicadores, referentes a los controles para la seguridad de la información, implementados por la empresa.

Si requiere más información puede comunicarse con nosotros(as), William García Molina, cédula 6-0436-0917 y Michelle Rodríguez Hernández, cédula 6-0455-0898, estudiantes activos de la Universidad Técnica Nacional (UTN), Teléfonos: 8486-9786 /8721-2517 y a los correos electrónicos: wsgarciamo@est.utn.ac.cr / merodriguezher@est.utn.ac.cr

Yo_____, portador del número de cédula de identidad _____, luego de leer y comprender todos los detalles de esta investigación _____, estoy de acuerdo con mi participación en el proyecto.

Firma_____

Cédula_____

Yo _____, número de cédula_____, como testigo de la firma de este contrato de consentimiento, afirmo que leí y comprendí el documento en su totalidad.

Firma_____

UNIVERSIDAD TÉCNICA NACIONAL

LICENCIATURA EN INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN

ANALIZAR LOS CONTROLES PARA LA SEGURIDAD DE LA INFORMACIÓN IMPLEMENTADOS POR LA EMPRESA DISTRIBUIDORA COARSA, EN SAN RAMÓN DE ALAJUELA, DE ACUERDO CON LA NORMA ISO 27002, DURANTE EL SEGUNDO SEMESTRE DEL AÑO 2022

INSTRUMENTO DE RECOLECCIÓN DE INFORMACIÓN

La presente lista de cotejo tiene como finalidad, verificar si la empresa “Distribuidora COARSA” cumple con las pautas que se encuentran en el Capítulo VII de la Norma ISO 27002:2022, el cual tiene como título “Controles Físicos”. Los resultados obtenidos se analizarán, con el fin de crear una política de seguridad para la organización.

Así mismo, para analizar los resultados de este instrumento, se utilizará la siguiente escala: Bajo (1) Medio (2) Alto (3)

Con base en el promedio obtenido en cada control, se determinará el nivel de cumplimiento de cada uno.

LISTA DE COTEJO: CONTROLES FÍSICOS

Perímetros de seguridad física **Objetivo:** evitar el acceso físico no autorizado, el daño y la interferencia a la información de la organización y otros activos asociados.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
01	¿Los edificios que contienen instalaciones de procesamiento de información cuentan con perímetros solidos (es decir, no hay espacios o áreas donde un robo pueda ocurrir fácilmente)?	2	A pesar de que se cuenta con perímetros físicamente sólidos, algunas zonas como la recepción son abiertas, además, existen zonas donde no se ve ningún tipo de seguridad, como escritorios de uso público.
02	¿Los techos, paredes y pisos de las instalaciones de la empresa, son de construcción sólida?	3	
03	¿Las puertas exteriores y ventanas están adecuadamente protegidas contra el acceso no autorizado con mecanismos de	2	Las ventanas y puertas están debidamente aseguradas, pero no hay presencia de alarmas.

	control (por ejemplo, rejas, alarmas, cerraduras)?		
04	¿Las puertas contra incendios son revisadas constantemente por el personal a cargo?	1	A pesar de que existe una brigada, no se hacen revisiones constantes.
Promedio		2	**Nivel de cumplimiento:** Medio
Entrada Física **Objetivo:** garantizar solo el acceso físico autorizado a la información de la organización y otros activos asociados.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
05	¿El acceso a los sitios y edificios se le permite solo al personal autorizado?	3	Al acceder a la empresa es necesario brindarle los datos personales al guarda de seguridad, además, todos los funcionarios cuentan con gafete.
06	¿El personal encargado de las áreas donde se procesa información confidencial, cuenta con un libro o registro físico o electrónico de auditoría	3	Se cuenta con varios registros por medio de libros en las áreas más importantes.

	donde se registran todos los accesos?		
07	¿Existen mecanismos técnicos para la gestión del acceso a las áreas donde se procesa o almacena la información, es decir, tarjetas de acceso, biometría o autenticación de dos factores?	3	La totalidad de los funcionarios cuentan con gafete.
08	¿Hay establecida un área de recepción supervisada por personal u otros medios para controlar el acceso físico a el sitio o edificio?	3	En la entrada del edificio hay una caseta de guardas con el respectivo funcionario.
09	¿El personal de seguridad inspecciona las pertenencias de los funcionarios y de personas externas al ingresar o salir de las instalaciones de la empresa?	2	Al salir únicamente, en el caso de los carros se revisa la cajuela y se les solicita que bajen las ventanas.

10	¿El personal y las partes interesadas usan algún tipo de identificación visible con insignias fácilmente distinguibles e identifican a los empleados permanentes, proveedores y visitantes?	1	Al entrar casi nunca usan el gafete, pero se identifican con el uniforme.
11	¿Se les otorga a personas externas a la empresa el acceso a zonas restringidas, únicamente en los casos estrictamente necesarios?	3	
12	¿Las áreas de carga y descarga están diseñadas para que las entregas puedan cargarse y descargarse sin personal de entrega que obtiene acceso no autorizado a otras partes del edificio?	2	No, pero hay una persona monitoreando todo el proceso.
13	¿Se inspecciona y examina las entregas entrantes en busca de explosivos, productos químicos	1	El personal encargado considera que no es necesario,

	u otros materiales peligrosos antes de que se muevan de las áreas de entrega y carga?		porque lo más tóxico que se usa son desinfectantes.
14	¿Se separan físicamente tanto los envíos entrantes como salientes y se inspeccionan las entregas que ingresan, en busca de evidencia de manipulación en el camino?	3	Se realizan aproximadamente tres verificaciones por parte de distintos funcionarios.
Promedio		2	**Nivel de cumplimiento:** Medio
Seguridad de oficinas, salas e instalaciones **Objetivo:** prevenir el acceso físico no autorizado, el daño y la interferencia a la información de la organización y otros activos asociados en las oficinas, salas e instalaciones.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
15	¿Las oficinas que se consideran de acceso restringido, están ubicadas en lugares de difícil acceso para el público?	3	En el caso de las dos zonas que se consideran las más críticas, las cuales son el centro de datos y la zona de chequeo de mercadería, se encuentran en zonas estratégicas que se consideran seguras, en el caso

			específico del centro de datos, se encuentra ubicado en una zona segura con llave, pero la puerta es de cristal transparente, por lo tanto, aún se puede ver parcialmente.
16	¿Las zonas en donde se procesa información son discretas, es decir, no hay presencia de señalización que indique el tipo de actividad que se realiza?	3	Las zonas más críticas no cuentan con ningún tipo de señalización.
17	¿Las instalaciones de la empresa brindan la privacidad suficiente, es decir, las actividades privadas no son visibles ni audibles?	2	En el caso de la visibilidad, la empresa cuenta con paredes de vidrio totalmente transparentes, para el caso del sonido, las conversaciones son totalmente indistintas.
18	¿Las guías telefónicas y mapas de zonas de la empresa, no se ponen a disposición de	3	

	cualquier persona, es decir son confidenciales?		
Promedio		3	**Nivel de cumplimiento:** Alto
Protección contra amenazas físicas y ambientales **Objetivo:** prevenir o reducir las consecuencias de eventos originados por amenazas físicas y ambientales.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
19	¿La ubicación y construcción de las instalaciones tomaron en cuenta la topografía local, como elevación adecuada, masas de agua, fallas tectónicas y amenazas urbanas?	3	
20	¿La empresa cuenta con sistemas capaces de detectar incendios o inundaciones en una etapa temprana para evitar que el fuego o el agua dañen los medios de almacenamiento y los dispositivos relacionados, como, por ejemplo, los sistemas	2	Únicamente alarmas de incendios.

	de procesamiento de información?		
21	¿La empresa cuenta con sistemas capaces de proteger los sistemas de información tanto del servidor como del cliente contra sobretensiones eléctricas o eventos similares para minimizar las consecuencias de tales eventos?	3	
22	¿Se llevan a cabo inspecciones aleatorias para detectar explosivos o armas en el personal, vehículos o mercancías que ingresan a las instalaciones de procesamiento de información confidencial?	1	Se hacen revisiones únicamente al entrar o salir de la empresa y lo mismo aplica para la entrada y salida de mercadería.
Promedio		2	**Nivel de cumplimiento:** Medio
Trabajar en áreas seguras			

Objetivo: proteger la información y otros activos asociados en áreas seguras contra daños e interferencias no autorizadas por parte del personal que trabaja en estas áreas.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
23	¿Se informa al personal sobre la existencia de actividades dentro de un área segura solo cuando es realmente necesario?	3	Al momento de realizar esta lista, se le informó al personal por medio de un grupo de WhatsApp, igualmente en el caso de la encuesta.
24	¿Se evita siempre que sea posible el trabajo sin supervisión en áreas seguras tanto por razones de seguridad como para reducir las posibilidades de actividades maliciosas?	3	Todas las zonas seguras se protegen con llaves.
25	¿Se llevan a cabo inspecciones periódicas en áreas seguras vacantes?	3	Las zonas vacantes y sin uso se encuentran protegidas con llave. Pero cuando es necesario se autoriza.
26	¿Está prohibido utilizar equipos fotográficos, de video, de audio u otros equipos de grabación,	3	

	incluyendo dispositivos terminales?		
27	¿Está siendo controlado adecuadamente el transporte y uso de los dispositivos de punto final del usuario en áreas seguras?	3	Se utiliza una boleta, pero no es muy necesario.
28	¿Se publican los procedimientos de emergencia de manera fácilmente visible o accesible?	1	No existe un repositorio publico donde puedan acceder.
Promedio		3	**Nivel de cumplimiento:** Alto
Escritorio y pantalla despejados **Objetivo:** reducir los riesgos de acceso no autorizado, pérdida y daño de la información en escritorios, pantallas y en otros lugares accesibles durante y fuera del horario normal de trabajo.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
29	¿Se protege la información comercial confidencial o crítica cuando no se requiere y especialmente cuando el cargo quede vacante?	3	No existe un procedimiento documentado, pero si se realiza un debido proceso en los casos de despido, que incluye revisiones de los dispositivos que utilizaba el funcionario.

30	¿Están protegidos los dispositivos de punto final del usuario mediante cerraduras con llave u otros medios de seguridad cuando no están en uso?	3	
31	¿Se dejan los dispositivos de punto final de usuario desconectados o protegidos con un mecanismo de bloqueo de pantalla cuando están desatendidos?	3	Las máquinas están configuradas para bloquearse después de un tiempo, además, los usuarios deben cambiar la contraseña frecuentemente.
32	¿Las impresoras cuentan con una función de autenticación, de modo que los creadores son los únicos que pueden obtener sus impresiones?	3	Sí, los usuarios deben ingresar un código único de cada uno para poder imprimir.
33	¿Los documentos y medios de almacenamiento extraíbles que contienen información confidencial se almacenan de	3	Utilizan discos extraíbles y se encuentran bajo llave.

	manera segura y cuando ya no se necesitan?		
34	¿Se establecen y comunican reglas y orientación para la configuración de ventanas emergentes en las pantallas (ejemplo, desactivar las nuevas ventanas emergentes de correo electrónico y mensajería, si es posible, durante presentaciones, pantallas compartidas o en un área pública)?	1	Pero existen configuraciones a nivel de dominio para el caso de las notificaciones, USB, etc.
35	¿Se borra información sensible o crítica en pizarras y otros tipos de pantallas cuando ya no se necesita?	1	No se suele anotar información en pizarras.
Promedio		2	**Nivel de cumplimiento:** Medio
Ubicación y protección del equipo **Objetivo:** reducir los riesgos de amenazas físicas y ambientales, y de accesos y daños no autorizados.			
N.°	**Indicadores**	**Puntos**	**Observaciones**

36	¿La ubicación de los equipos evita el acceso innecesario a las áreas de trabajo, es decir, evitan el acceso no autorizado?	3	
37	¿Las instalaciones de procesamiento de información que manejan datos confidenciales están ubicadas cuidadosamente para reducir el riesgo de que información confidencial sea vista por personas no autorizadas durante su uso?	3	
38	¿Existen controles para minimizar el riesgo de posibles amenazas físicas y ambientales, por ejemplo, robo, incendio, explosivos, humo, agua o falla en el suministro de agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las	1	Únicamente existe una brigada que se encarga de rotular las zonas y minimizar riesgos.

	comunicaciones, radiación electromagnética y vandalismo?		
39	¿La empresa tiene establecidas reglas para comer, beber y fumar en la cercanía de las instalaciones donde se realiza procesamiento de información?	3	
40	¿Existe una constante monitorización de las condiciones ambientales, tales como la temperatura y la humedad, en busca de condiciones que puedan afectar negativamente el funcionamiento de las instalaciones de procesamiento de información?	2	Únicamente en la bodega.
41	¿Se aplica protección contra rayos a todos los edificios y se colocan filtros de protección contra rayos en todas las	1	

	entradas líneas eléctricas y de comunicaciones?		
42	¿Los equipos en ambientes industriales están protegidos con métodos especiales, como membranas de teclado?	3	Se utilizan únicamente en la bodega.
43	¿Se protege los equipos que procesan información confidencial para minimizar el riesgo de fuga de información debido a la emanación electromagnética?	3	
44	¿Se separan físicamente las instalaciones de procesamiento de información gestionadas por la organización de aquellas no gestionadas por la organización?	3	Los sistemas están totalmente separados uno del otro. En el caso de las instalaciones no.
Promedio		2	**Nivel de cumplimiento:** Medio

Seguridad de los activos fuera de las instalaciones

Objetivo: evitar la pérdida, el daño, el robo o el compromiso de los dispositivos externos y la interrupción de las operaciones de la organización.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
45	¿Los equipos retirados de las instalaciones por motivos laborales, son protegidos de manera adecuada, es decir, no se dejan desatendidos en ningún momento?	3	
46	¿Se observan las instrucciones del fabricante para proteger el equipo en todo momento (por ejemplo, protección contra exposición a fuertes campos electromagnéticos, agua, calor, humedad, polvo)?	3	Se protegen contra daños y se colocan UPS a los equipos para protegerlos de campos electromagnéticos.
47	Cuando se transfieren equipos fuera de las instalaciones entre diferentes personas o partes interesadas, ¿se mantiene un registro que define la cadena de custodia del equipo, incluidos al	3	

	menos los nombres y las organizaciones de quienes son responsables del equipo, la información que no necesita transferirse con el activo se elimina de forma segura antes de la transferencia?		
48	Cuando es necesario y práctico, ¿se solicita autorización para retirar equipos y medios de las instalaciones de la organización para mantener un registro de tales retiros que facilite la justificación de incidentes en caso de una posible auditoría?	3	Se utiliza una boleta para retirar o transportar los equipos.
49	¿Se protege la visualización de información en un dispositivo (por ejemplo, móvil o portátil) en el transporte público?	3	Se utiliza autentificación de dos factores y los usuarios utilizan únicamente vehículos propios y de la empresa.
50	¿El personal de Tecnologías de Información implementa algún tipo de seguimiento y borrado	1	Se realiza por medio de Google, pero una medida propia de la

	remoto en caso de pérdida de dispositivos por parte de funcionarios?		empresa. Por lo tanto, no es necesario.
Promedio		3	**Nivel de cumplimiento:** Alto
Medios de almacenamiento **Objetivo:** garantizar solo la divulgación, modificación, eliminación o destrucción autorizadas de la información almacenada.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
51	¿La empresa cuenta con una política sobre la gestión de medios de almacenamiento extraíbles y se comunica dicha política específica a cualquier persona que use o manipule medios de almacenamiento extraíble?	1	Solamente TI y Gerencia, por lo tanto, no es necesario. Pero sí es necesario que los usuarios tengan conocimiento.
52	Cuando es necesario y práctico, ¿se solicita autorización para que los medios de almacenamiento se retiren de la	3	

	organización y para mantener un registro de tales retiros en caso de una auditoría?		
53	¿Los medios de almacenamiento extraíbles se almacenan en un entorno seguro?	3	
54	¿Se mitiga el riesgo de que los medios de almacenamiento se degraden mientras aún se necesita la información almacenada, transfiriendo la información a nuevos medios de almacenamiento antes de volverse ilegible?	3	Sí, pero la información se encuentra en múltiples dispositivos. Por lo tanto, no es necesario pasarlo de uno a otro de manera urgente.
55	¿Se almacenan múltiples copias de información valiosa en medios de almacenamiento separados para reducir aún más el riesgo de daño o pérdida de información coincidente?	3	Sí, la información se almacena en múltiples medios de almacenamiento.

56	¿Se habilitan puertos de medios de almacenamiento extraíbles [por ejemplo, ranuras para tarjetas *Secure Digital* (SD) y serie universal, puertos de bus (USB)] únicamente si existe una razón organizativa para su uso?	1	Nunca ha sido necesario habilitarlos.
57	Cuando es necesario utilizar medios de almacenamiento extraíbles, ¿se monitorea la transferencia de información a tales medios de almacenamiento?	1	No están habilitados los puertos.
58	Si los medios de almacenamiento que contienen información confidencial deben reutilizarse dentro de la organización, ¿se eliminan los datos de forma segura o se formatean los medios de almacenamiento antes de reutilizarlos?	3	Se les entregan a los encargados de reciclaje de la Municipalidad, los cuales le realizan un debido proceso.

59	Al utilizar servicios de recogida y eliminación de medios de almacenamiento, ¿se verifica que el proveedor sea de confianza?	3	
60	¿Se registra la eliminación de elementos sensibles para mantener un registro de auditoría?	3	Se realiza un correo con datos como el número de serie, se valida con Gerencia y Contabilidad y, por último, se procede a desechar.
Promedio		2	**Nivel de cumplimiento:** Medio

Utilidades de apoyo **Objetivo:** evitar la pérdida, el daño o el compromiso de la información y otros activos asociados o la interrupción de las operaciones de la organización debido a fallas e interrupciones de los servicios públicos de apoyo.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
61	¿El personal de Tecnologías de Información se asegura de que el equipo de apoyo a los servicios públicos esté configurado, operado y mantenido de acuerdo con las especificaciones del fabricante correspondiente?	1	Las instalaciones no lo requieren.
62	¿Se garantiza que las empresas de servicios públicos sean evaluadas regularmente por su capacidad para satisfacer el crecimiento y las interacciones comerciales con otras utilidades de apoyo?	1	Solamente se evalúa el servicio de Internet.
63	¿El personal de Tecnologías de Información se asegura de que		Se garantiza que los cableados sean subterráneos hasta llegar

	el equipo de apoyo a los servicios públicos esté en una red separada del procesamiento de información si está conectado a una red, además, se aseguran de que estén conectados a Internet solo cuando sea necesario y solo de manera segura?	1	a la *data center*, los módems en la parte del *wifi* está bloqueado, los usuarios TI controlan el acceso, ya sean por redes inalámbricas o cableado.
Promedio		1	**Nivel de cumplimiento:** Bajo
Seguridad del cableado **Objetivo:** evitar la pérdida, el daño, el robo o el compromiso de la información y otros activos asociados y la interrupción de las operaciones de la organización relacionadas con el cableado de energía y comunicaciones.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
64	¿Las líneas eléctricas y de telecomunicaciones a las instalaciones de procesamiento de información son subterráneas cuando sea posible o están sujetas a una		Los cables de datos y los eléctricos son subterráneos en la medida de lo posible.

	protección alternativa adecuada, como protectores de cables en el piso y postes de servicios públicos?, si los cables son subterráneos, ¿se protegen de cortes accidentales (por ejemplo, con conductos blindados o señales de presencia)?	3	
65	¿Los cables de alimentación de comunicaciones están separados para evitar interferencias?	3	
66	¿Los cables están etiquetados en cada extremo con suficientes detalles de origen y destino para permitir la identificación física y la inspección del cable?	3	
Promedio		3	**Nivel de cumplimiento:** Alto
Mantenimiento de equipos			

Objetivo: evitar la pérdida, daño, robo o compromiso de la información y otros activos asociados y la interrupción de las operaciones de la organización causada por la falta de mantenimiento.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
67	¿Los equipos informáticos son utilizados hasta el fin de la vida útil recomendada por el fabricante?	1	Se utilizan hasta que fallen.
68	¿La empresa cuenta con un programa de mantenimiento?	1	
69	¿Solo el personal de mantenimiento autorizado realiza reparaciones y mantenimiento a los equipos?	2	Depende de la gravedad y el nivel de complicación que implique. Se podría decir que un 90% se realiza en la empresa.
70	¿Se mantiene un registro de todas las fallas sospechadas o reales y de todo mantenimiento preventivo y correctivo?	1	Cuentan con un plan remedial, un sistema para control de fallos, para conocer los tiempos fuera.
71	¿Se implementan controles apropiados cuando el equipo esté programado para		El personal de la empresa lo hace.

	mantenimiento, teniendo en cuenta si este mantenimiento es realizado por personal en el sitio o externo a la organización? ¿se somete al personal de mantenimiento a un adecuado acuerdo de confidencialidad?	1	
72	¿El mantenimiento remoto se realiza por medio de algún tipo de autorización?	3	Es el más común. Existe un *chat* de soporte para que indiquen su caso. Ellos deben brindar un código y se debe autorizar.
73	¿Antes de volver a poner en funcionamiento el equipo después del mantenimiento, se inspecciona para asegurarse de que el equipo no ha sido manipulado y funciona correctamente?		Sí, se realiza mediante un perfil de soporte que se le brinda al usuario que reparó.
Promedio		1	**Nivel de cumplimiento:** Bajo
Eliminación segura o reutilización de equipos			

Objetivo: evitar la fuga de información de los equipos que se desecharán o reutilizarán			
N.°	**Indicadores**	**Puntos**	**Observaciones**
74	Los medios de almacenamiento que contienen información confidencial o con derechos de autor ¿se destruyen físicamente o la información se elimina o sobrescribe utilizando técnicas para hacer que la información original no se pueda recuperar en lugar de utilizar la función de eliminación estándar?	3	Se retiran los medios de almacenamiento en caso de desecharse algún equipo que lo contenga. Además, se aseguran de que los datos no se puedan recuperar.
75	Las etiquetas y marcas que identifiquen a la organización o que indiquen la clasificación, el propietario, el sistema o la red ¿se eliminan antes de desecharse, incluida la reventa o la donación a organizaciones benéficas?	1	La empresa no participa en causas benéficas.
Promedio		2	**Nivel de cumplimiento:** Medio

Anexo 6: Lista de cotejo de controles tecnológicos

UNIVERSIDAD TÉCNICA NACIONAL, SEDE DEL PACÍFICO

LICENCIATURA EN INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN

ANALIZAR LOS CONTROLES PARA LA SEGURIDAD DE LA INFORMACIÓN IMPLEMENTADOS POR LA EMPRESA DISTRIBUIDORA COARSA, EN SAN RAMÓN DE ALAJUELA, DE ACUERDO CON LA NORMA ISO 27002, DURANTE EL SEGUNDO SEMESTRE DEL AÑO 2022

FÓRMULA DE CONSENTIMIENTO INFORMADO

Lista de cotejo para verificar el cumplimiento de los controles tecnológicos de la Norma ISO 27002:2022 por parte de la empresa Distribuidora COARSA

Estimados (as) señores(as):

Esta lista de cotejo tiene como finalidad recopilar la información necesaria que será utilizada para elaborar un proyecto de graduación sobre los controles para la seguridad de la información implementados por la empresa Distribuidora COARSA, en San Ramón de Alajuela, de acuerdo con la Norma ISO 27002:2022, durante el segundo semestre del año 2022.

Se solicita su colaboración para contestar algunos indicadores, referentes a los controles para la seguridad de la información, implementados por la empresa.

Si requiere más información puede comunicarse con nosotros(as), William García Molina, cédula 6-0436-0917 y Michelle Rodríguez Hernández, cédula 6-0455-0898, estudiantes activos de la Universidad Técnica Nacional (UTN), Teléfonos: 8486-9786 /8721-2517 y a los correos electrónicos: wsgarciamo@est.utn.ac.cr / merodriguezher@est.utn.ac.cr

Yo_____, portador del número de cédula de identidad _____, luego de leer y comprender todos los detalles de esta investigación _____, estoy de acuerdo con mi participación en el proyecto.

Firma_____

Cédula_____

Yo _____, número de cédula_____, como testigo de la firma de este contrato de consentimiento, afirmo que leí y comprendí el documento en su totalidad.

Firma_____

UNIVERSIDAD TÉCNICA NACIONAL

LICENCIATURA EN INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN

ANALIZAR LOS CONTROLES PARA LA SEGURIDAD DE LA INFORMACIÓN IMPLEMENTADOS POR LA EMPRESA DISTRIBUIDORA COARSA, EN SAN RAMÓN DE ALAJUELA, DE ACUERDO CON LA NORMA ISO 27002, DURANTE EL SEGUNDO SEMESTRE DEL AÑO 2022

INSTRUMENTO DE RECOLECCIÓN DE INFORMACIÓN

La presente lista de cotejo tiene como finalidad, verificar si la empresa “Distribuidora COARSA”, cumple con las pautas que se encuentran en el Capítulo VIII de la Norma ISO 27002:2022, el cual tiene como título “Controles Tecnológicos”. Los resultados obtenidos se analizarán con el fin de crear una política de seguridad para la organización.

Así mismo, para analizar los resultados de este instrumento, se utilizará la siguiente escala: Bajo (1) Medio (2) Alto (3)

Con base en el promedio obtenido en cada control, se determinará el nivel de cumplimiento de cada uno.

LISTA DE COTEJO: CONTROLES TECNOLÓGICOS

Dispositivos de punto final **Objetivo:** Proteger la información contra los riesgos introducidos por el uso de dispositivos de punto final de usuario.			
Políticas del uso del dispositivo			
N.°	**Indicadores**	**Puntos**	**Observaciones**
01	¿Existen políticas en cuanto al tipo de información y el nivel de clasificación que se procesa, almacena o soporta?	1	
02	¿Se registran los dispositivos de punto final?	3	Existen registros de todos los dispositivos de la empresa, por número de serie, propietario etc.
03	¿Existen requisitos para la protección física?	1	
04	¿Se tiene restricciones en cuanto al software que puede instalarse?	3	A nivel de *active directory* existen una serie de restricciones que implican la

			prohibición de instalación de software.
05	¿Hay requisitos para la instalación y actualización del software?	3	
06	¿Existen reglas en cuanto a las conexiones a servicios de información, redes públicas o cualquier red que se encuentra fuera de las instalaciones?	1	No se utilizan redes fuera de la empresa.
07	¿Existen controles de acceso?	2	Existen ciertas reglas a nivel de *active directory*.
08	¿Los dispositivos de almacenamiento se encuentran cifrados?	2	Los dispositivos extraíbles no cuentan con cifrado.
09	¿Existen protecciones contra el malware?	3	Cuentan con el software Eset EndPoint Security
10	¿Se puede deshabilitar, borrar o bloquear de forma remota dispositivos de la empresa que se hayan extraviado?	2	No existe una aplicación o sistema que permita el borrado o bloqueo remoto, únicamente las

			brindadas por el fabricante.
11	¿Se realizan copias de seguridad?	3	Tanto a nivel de servidores como en dispositivos de almacenamiento extraíbles.
12	¿Existen políticas en cuanto al uso de servicios web y aplicaciones web?	2	Existen únicamente restricciones a nivel de *active directory*.
13	¿Se realizan análisis del comportamiento del usuario final?	1	
14	¿Se puede hacer uso de dispositivos extraíbles, incluyendo las memorias extraíbles, así como desactivar puertos físicos?	3	Los puertos están deshabilitados en la totalidad de los equipos y nunca ha sido necesario habilitarlos.
15	¿Se puede hacer de uso de capacidades de partición, siendo compatible con el dispositivo de punto final del usuario,	1	

	efectuándose de forma segura la información de la empresa y otros activos asociados?		
16	¿El usuario puede cerrar su sesión y cancelar los servicios que no se utilizan?	3	
17	Los dispositivos que no se están usando, ¿se protegen para evitar el uso no autorizado por medio de un control físico y un control lógico?	3	Los usuarios que abandonan su área bloquean el dispositivo. Igualmente, en el caso de un equipo que no esté en uso.
18	¿Se tiene cuidado al hacer uso del dispositivo en sitios públicos, oficinas abiertas, sitios de reuniones, entre otras áreas desprotegidas?	3	
19	¿Los dispositivos cuentan con seguros de protección contra robo?	1	
20	¿Se realiza una separación del uso personal y comercial de los dispositivos, incluyendo el uso de software para	1	No se utilizan dispositivos personales para uso laboral.

	respaldar y proteger los datos comerciales en un dispositivo privado?		
21	¿Solo se brinda acceso a la información a los usuarios que hayan reconocido sus labores, renuncien a la propiedad de datos comerciales, otorguen permisos de borrado de datos de forma remota, en caso de requerirse?	1	No se realiza borrado de datos remoto.
22	¿Se tiene políticas y procedimientos específicos del tema para prevenir disputas relacionadas con los derechos de propiedad intelectual desarrollados en equipos de propiedad privada?	1	
23	¿Se tiene acceso a equipos de propiedad privada que se pueden prevenir por la legislación?	1	
24	¿Se tiene acuerdos de licencias de software que la misma organización se puede hacer responsable de la concesión de licencias para el software de cliente de	2	La empresa cuenta con las licencias respectivas del software que utiliza, a excepción de la

	usuario de propiedad privada del personal o usuario externo?		licencia de Microsoft Windows 10, la empresa los tiene activados de manera ilegal.
25	¿Existe un procedimiento de la configuración de conexiones inalámbricas?	3	Se utiliza una autenticación de doble factor que consiste en ingresar la contraseña de la red para autenticarse seguidamente mediante un usuario y contraseña.
26	¿Se hace uso de las conexiones inalámbricas o alámbricas con el ancho de banda adecuado a las políticas?	3	Se hace, pero no existe una documentación o políticas para ello.
Promedio		2	**Nivel de cumplimiento:** Medio

Derechos de acceso privilegiado **Objetivo:** garantizar que solo los usuarios autorizados, los componentes y servicios de software reciban derechos de acceso privilegiado.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
27	Se tiene identificados los usuarios que requieren de derechos de acceso privilegiado para cada sistema o proceso.	3	
28	Se asignan los derechos de acceso privilegiado a los usuarios según se considere necesario.	3	
29	Existe un administrador o algún proceso de autorización para la otorgación de derechos privilegiados, así como un registro de los que se han asignado.	3	
30	Se definen e implementan requisitos para el vencimiento de los derechos de acceso privilegiado.	1	No vencen y no se definen requisitos.

31	Los usuarios conocen de los derechos de acceso privilegiados con los que cuentan, y cuándo los están usando.	2	Si lo conocen, pero lo toman como algo en función de su puesto.
32	Los requisitos para la autenticación de usuarios con derechos de acceso privilegiado son mayores en cuanto a los usuarios con otros niveles de acceso.	2	Tienen las mismas características que las de usuarios menos privilegiados.
33	Se realizan revisiones a los usuarios que poseen derechos de acceso privilegiado para verificar que sus permisos aún califiquen para mantener el rol, esto después de cualquier cambio organizacional o revisiones periódicas.	1	
34	Existen reglas específicas para que no se haga uso del usuario *root*, administrando y protegiendo la información de autenticaciones con esta identidad.	3	

35	Se otorga acceso privilegiado de manera temporal, en el tiempo necesario para la implementación de cambios o actividades que se aprobaron.	3	En los casos en los que fue necesario.
36	Se registran todos los accesos privilegiados.	3	Se mantiene una lista de accesos y nombres.
37	Los derechos de acceso privilegiado no se comparten o vinculan a más de una persona.	3	
38	Los derechos de acceso privilegiado se otorgan para tareas administrativas.	3	
Promedio		3	**Nivel de cumplimiento:** Alto
Restricción de acceso a la información **Objetivo:** garantizar solo el acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados.			
Requisitos			
N.°	**Indicadores**	**Puntos**	**Observaciones**

39	Los usuarios con identidades desconocidas no pueden acceder a información sensible.	3	
40	Se proporcionan mecanismos de configuración para el control de acceso a la información en sistemas, aplicaciones y servicios.	3	Existen mecanismos para configurar aplicaciones y servicios de acuerdo con el departamento.
41	Se controla el tipo de datos a los que el usuario particular pueden acceder.	3	
42	Controlan los tipos de usuarios que se le asignan distintos roles.	3	
43	Proporcionan controles de acceso físico o lógicos para el aislamiento de aplicaciones sensibles, de datos o sistemas.	3	
44	Poseen un control granular sobre quién tiene acceso a la información, así como el periodo y la manera en que acceden.	3	

45	Mantienen un control sobre quiénes pueden compartir información con personas ajenas a la institución.	3	Se comparten datos por medio de una máquina virtual con escritorio remoto, pero el acceso es limitado, únicamente se tiene acceso a los archivos necesarios.
46	Se gestiona de forma dinámica, en tiempo real, el uso y distribución de la información.	3	Se realizan reportes y se pueden consultar por medio de un software.
47	Se tiene protección de la información para evitar cambios no autorizados, realización de copias y distribución.	3	
48	Se monitorea el uso de la información.	3	Por medio de un software.

49	Registran los cambios efectuados en la información que tenga lugar, en caso de que se lleve una investigación futura.	1	
50	Se otorga permisos de acceso de acuerdo con la función de la identidad, el dispositivo, ubicación o la aplicación.	3	
51	Aprovechan el esquema de clasificación para determinar qué información requiere de protección con técnicas de gestión de acceso dinámico.	1	
52	Se establecen procesos operativos, de seguimiento y presentación de informes, así como apoyo técnico para infraestructura.	1	No es relevante para la empresa.
53	La autenticación, las credenciales apropiadas o un certificado para acceder a la información es exigida.	3	Los funcionarios que requieren el uso de tecnología cuentan con un usuario y contraseña.

54	El acceso se restringe de acuerdo con las políticas establecidas.	3	
55	Se cifra la información.	1	
56	Existen permisos definidos en cuanto a la impresión de la información.	2	La mayoría cuenta con permiso para imprimir.
57	Se registra quién accede a la información y el uso que le da.	1	
58	Si se detecta intentos de uso inadecuado de la información, se alarma inmediatamente.	3	Se reporta a los jefes directos.
Promedio		2	**Nivel de cumplimiento:** Medio

Acceso al código fuente

Objetivo: evitar la introducción de funciones no autorizadas, evitar cambios no intencionales o maliciosos y mantener la confidencialidad de la propiedad intelectual valiosa.

N.°	Indicadores	Puntos	Observaciones
59	De acuerdo con los procedimientos establecidos, se administra el acceso al código fuente y a las bibliotecas fuentes del programa.	1	Solamente el personal de TI tiene acceso a los códigos fuente.
60	Se conceden permisos de lectura y escritura al código fuente en función a las necesidades empresariales y gestionado para abordar riesgos de alteración y mal uso.	3	Únicamente al personal de TI.
61	Se efectúan los cambios en el código fuente, con una previa autorización por parte del propietario del código fuente.	1	Se manipula mayormente las bases de datos.
62	Se le deniega el acceso directo al repositorio de código fuente, solo pueden acceder a través de herramientas para desarrollados que son capaces de controlar las actividades y autorizaciones sobre el código.	1	

63	Se mantiene un listado de programas en un entorno seguro, en el cual los accesos de lectura y escritura puedan ser administrados y asignados.	1	
64	Tienen un registro de auditoría de todos los accesos y cambios en el código fuente.	1	
Promedio		1	**Nivel de cumplimiento:** Bajo
Autenticación segura **Objetivo:** garantizar que un usuario o una entidad se autentica de forma segura cuando se otorga acceso a sistemas, aplicaciones y servicios.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
65	Se muestra la información confidencial hasta que se haya iniciado sesión de forma completa.	3	
66	Se muestra un aviso donde indica que solo personal autorizado puede acceder al sistema o servicio.	1	

67	Se realiza el inicio de sesión sin mensajes específicos de ayuda.	1	
68	Existe protección contra intentos de inicio de sesión de fuerza bruta.	1	
69	Solamente se validan los datos de entrada cuando están completos.	3	Se deben cumplir ciertos requisitos, por ejemplo diez caracteres, números y letras.
70	Se registra la cantidad de ingresos fallidos y exitosos.	1	
71	Al existir un inicio de sesión forzado se detecta inmediatamente y se genera un evento de seguridad.	3	Mediante el *active directory*. Por un software específico.
72	Se muestra o envía información por canales separados en caso de: - Fecha y hora de inicio de sesión exitosa. - Detalles de inicio de sesión fallidos desde la última vez que se logró acceder sin fallas.	2	Solamente en el *active directory*.

73	La contraseña se muestra en la pantalla de forma cifrada.	3	
74	Las contraseñas no se transmiten sin cifrar a través de una red.	3	
75	Las sesiones después de encontrarse sin actividad por un tiempo, se cierra sesión de forma automática.	3	
76	Los tiempos de duración de la conexión son restringidos.	3	
Promedio		2	**Nivel de cumplimiento:** Medio
Protección contra software malicioso **Objetivo:** garantizar que la información y otros activos asociados estén protegidos contra malware			
N.°	Indicadores	Puntos	Observaciones
77	Hay reglas y controles implementados que prevengan o detecten el uso de software no deseado.	3	Por medio del *active directory* en el caso de las PC y

			mediante software en el caso de las tabletas.
78	Se tiene implementados controles que prevengan o detecten el uso de sitios web maliciosos, ya sea conocidos o sospechosos.	3	Se cuenta con un *firewall*, pero no está funcionando a su máxima capacidad.
79	Se han reducido las vulnerabilidades que pueden ser explotadas por *malware*.	2	Se utiliza Eset Endpoint Security.
80	Se realizan validaciones automatizada y periódicamente del software, así como del contenido de datos de los sistemas, sobre todo aquellos de procesos comerciales críticos.	3	Mediante el Eset Endpoint Security.
81	Se establecen medidas de protección contra los riesgos asociados con la obtención de archivos y software, tanto de redes externas u otros medios.	1	A pesar de que existen herramientas como el *firewall*, no se

			utilizan en su totalidad.
82	Se instala y actualiza regularmente el software de detección y reparación de *malware* para escaneo de computadores y medios de almacenamiento electrónicos.	3	Si, mediante Eset Endpoint Security.
83	Se determina la ubicación y configuración de las herramientas de detección y reparación de *malware*, en función del riesgo que dio como resultado de las evaluaciones previas.	3	Todas las máquinas cuentan con Eset Endpoint.
84	Se cuenta con protección contra la introducción de *malware* durante los mantenimientos del sistema y aplicaciones y en casos de emergencias con los que pueden eludirse los controles normales.	3	
85	Se implementan procesos de autorización para la desactivación temporal o permanente de algunas o todas las medidas contra el *malware*, incluyendo las	1	No existe, pero el personal del TI considera que es necesario.

	autoridades de aprobación de excepciones, justificación documentada y fechas de revisión.		
86	Se cuenta con planes apropiados de continuidad comercial para la recuperación en caso de ataques de *malware*, copias de seguridad de datos y software.	1	Por el momento no, pero el personal considera que es necesario.
87	Se aíslan ambientes más probables a una consecuencia catastrófica.	3	Tanto de manera física como lógica se aíslan ambientes de mayor vulnerabilidad.
88	Definen procedimientos y responsabilidad para el tratamiento de protección contra software malicioso en los sistemas, capacitación de uso, informes y recuperación de ataques de *malware*.	1	

89	Los colaboradores de la empresa reciben capacitaciones sobre cómo identificar y mitigar potencialmente la recepción, envió o instalación de correos electrónicos, archivos o programas infectados.	1	Se realizan avisos y se envían imágenes, pero una capacitación como tal, no.
90	Se recopila información regularmente sobre *malwares* nuevos, como suscripción a listas de correos o revisión de sitios web importantes.	3	Por medio de Eset.
91	Se verifica que la información obtenida provenga de fuentes calificadas y acreditadas.	1	Podría pasar, ya que no se controla.
Promedio		2	**Nivel de cumplimiento:** Medio

Gestión de vulnerabilidades técnicas **Objetivo:** prevenir la explotación de vulnerabilidades técnicas			
N.°	**Indicadores**	**Puntos**	**Observaciones**

92	Se definen y establecen funciones y responsabilidades asociadas a la gestión técnica de vulnerabilidades, como el monitoreo, evaluación de riesgos, actualizaciones, seguimientos de activos y cualquier otra responsabilidad de coordinación que se requiera.	2	Se revisa en algunas ocasiones.
93	Se identifican los recursos de información, utilizados para la identificación de vulnerabilidades técnicas relevantes, se actualiza la lista de acuerdo con los cambios en el inventario o cuando existen recursos nuevos o útiles.	1	Se maneja de memoria.
94	Se exige a los proveedores de sistemas de información que garanticen notificaciones, manejos y divulgación de vulnerabilidades, incluyendo los contratos.	1	No se les solicita.
95	Se hace uso de herramientas de escaneo de vulnerabilidades adecuadas para las	1	No se verifica. Ya que la empresa no cuenta con licencias

	tecnologías de identificación y verificación de un parcheo exitoso.		de algunos softwares como Windows y Office.
96	Se realizan pruebas de penetración planificadas, documentadas y repetibles, o evaluaciones por parte de personal competente y autorizada para respaldar la identificación de vulnerabilidades.	1	
97	Se rastrea el uso de bibliotecas de terceros o código fuente en busca de vulnerabilidades.	1	
98	Detectan la existencia de vulnerabilidades en sus productos y servicios, incluyendo componentes externos.	2	
99	Realizan y reciben informes de vulnerabilidades de fuentes internas o externas.	3	
100	Se verifica y analiza los informes para determinar qué respuesta y remediación se requiere.	1	

101	Al reconocer una vulnerabilidad técnica potencial, se efectúa la identificación de riesgos asociados y las acciones que se deben de llevar a cabo.	1	
102	Cuentan con un cronograma para reaccionar a las alarmas de vulnerabilidades potenciales, tomando medidas apropiadas y oportunas a la identificación de posibles vulnerabilidades técnicas.	3	Si existe, pero no está documentado.
103	Realizan el abordaje de la vulnerabilidad basada en los procedimientos de respuestas a incidentes de seguridad de la información.	1	Se necesita mejorar significativamente el cumplimiento de los procedimientos de seguridad para que el abordaje de la vulnerabilidad sea efectivo.
104	Las actualizaciones son de fuentes legítimas.	1	No se puede verificar, porque la empresa no cuenta con las

			licencias de algunos softwares como Office y Windows.
105	Antes de ejecutar una actualización, realizan pruebas fuera del entorno comercial para garantizar la efectividad y que no produzca efectos secundarios.	3	Sí, se realizan pruebas en entornos más aislados para evitar fallos.
106	Abordan los sistemas de alto riesgo de primero.	2	Existe una combinación de sistemas con diferentes niveles de riesgo.
107	Desarrollan soluciones a las vulnerabilidades técnicas.	1	
108	Realizan pruebas para confirmar que el parche o la solución brindada fue efectiva.	1	
109	Proporcionan mecanismos para verificar la autenticación de la solución.	1	
110	Si no se cuenta con alguna actualización o no se puede actualizar, se cuenta con	1	

	medidas extras para solucionar el problema.		
Promedio		1	**Nivel de cumplimiento:** Bajo
Gestión de la configuración **Objetivo:** garantizar que el hardware, el software, los servicios y las redes funcionen correctamente con la configuración de seguridad requerida y que esta no se altere por cambios no autorizados o incorrectos.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
111	Cuentan con orientación disponible de forma pública.	1	
112	Consideran el nivel de protección necesario para determinar el nivel suficiente de seguridad.	2	
113	Se respalda la política de seguridad de la información de la organización, políticas específicas del tema, estándares y otros requisitos de seguridad.	2	De manera parcial.

114	Consideran la factibilidad y aplicabilidad de las configuraciones de seguridad en el contexto organizacional.	3	
115	Se minimiza la cantidad de usuarios con derechos de acceso privilegiado o administrador.	3	Solo a el personal más importante como TI o Gerencia.
116	Se deshabilitan las identidades innecesarias que no se utilizan o sean inseguras.	1	
117	Se deshabilitan o restringen funciones y servicios no necesarios.	3	
118	Se restringe el acceso a programas de utilidades importantes y configuraciones de parámetros del *host*.	3	
119	Se sincronizan los relojes de todos los dispositivos.	3	
120	Se cambian las configuraciones predeterminadas, como contraseñas, usuarios, luego de la instalación y revisión de parámetros de seguridad.	3	

121	Se cierra automáticamente la sesión en los dispositivos informáticos luego de un periodo sin actividad.	3	
122	Se verifica que se haya cumplido con los requisitos de la licencia.	1	La empresa no cuenta con licencias para algunos softwares.
123	Se monitorean las configuraciones en conjunto de herramientas de administración del sistema.	3	
Promedio		2	**Nivel de cumplimiento:** Medio
Eliminación de información **Objetivo:** evitar la exposición innecesaria de información confidencial y cumplir con los requisitos legales, estatuarios y reglamentarios y contractuales para la eliminación de información.			
N.º	**Indicadores**	**Puntos**	**Observaciones**

124	Se selecciona el método adecuado basado en los requisitos comerciales, así como las leyes y regulaciones pertinentes.	1	No es relevante para la empresa.
125	Se registran los resultados de la eliminación como prueba.	3	Sí, pero únicamente por medio de una orden directa de los jefes.
126	Los proveedores que utilizan para el eliminado de información hacen entrega de la evidencia del borrado de información.	1	No utilizan proveedores para estos casos.
127	Se configuran los sistemas para que destruyan la información de manera segura, cuando no se necesite.	1	Solamente se elimina de manera manual.
128	Las versiones obsoletas, copias y archivos son eliminados por completo.	3	Se elimina información únicamente por medio de órdenes.

129	El software que utilizan para la eliminación de la información es seguro, aprobado y garantiza que no exista manera de recuperar la información.	1	No se utiliza.
130	Los proveedores que utilizan para la eliminación de la información se encuentran aprobados y certificados.	1	No se utilizan.
131	Se hace uso de mecanismos apropiados según el medio de almacenamiento que se desea eliminar la información.	3	
Promedio		2	**Nivel de cumplimiento:** Medio
Prevención de fuga de datos **Objetivo:** detectar y prevenir la divulgación y extracción no autorizada de información por parte de individuos o sistemas.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
132	Se identifica y clasifica la información para protegerla.	3	

133	Se monitorean los canales de fuga de datos.	3	
134	En caso de una fuga, se actúa inmediatamente para evitar la filtración de información.	3	
135	Se realiza una identificación y el monitoreo de información de carácter sensible que se encuentre en riesgo de una divulgación sin autorización.	3	Se realiza por medio del software Eset EndPoint Security.
136	Al darse una divulgación de información confidencial, se detecta inmediatamente.	1	Aún existen vulnerabilidades que deben tratarse.
137	Las acciones del usuario o transmisiones de la red que expongan información confidencial se bloquean automáticamente.	3	Por medio de un *firewall*.
Promedio		3	**Nivel de cumplimiento:** Alto
Copias de seguridad de la información			

Objetivo: permitir la recuperación de la pérdida de datos o sistemas.			
N.º	**Indicadores**	**Puntos**	**Observaciones**
138	Las copias de seguridad se registran de manera precisa y completa, realizando una restauración de procedimientos documentados.	3	
139	Las copias de seguridad reflejan los requisitos comerciales de la empresa, así como la frecuencia con la que se realizan.	2	Se realizan de acuerdo con la necesidad que el Departamento de TI considera.
140	Se almacenan en un lugar remoto, seguro y protegido, ante cualquier daño en el sitio principal.	3	Las copias de seguridad se almacenan en un lugar seguro, principalmente de los *data center*.
141	La información de respaldo recibe un nivel adecuado de protección física y ambiental.	3	

142	Se realizan de forma regular, pruebas en los medios que se utilizan para el respaldo de la información, con el fin de garantizar la confiabilidad, en casos de emergencias.	3	Las copias de seguridad se almacenan en un lugar seguro y se revisan constantemente.
143	Las copias de seguridad de la información se almacenan encriptadas, de acuerdo con los riesgos identificados.	1	No se utiliza ningún tipo de encriptación.
144	Antes de realizar una copia de seguridad, se asegura que no se detecte una pérdida inadvertida de los datos.	3	
Promedio		3	**Nivel de cumplimiento:** Alto

Redundancia de las instalaciones de procesamiento de información			
Objetivo: asegurar el funcionamiento continuo de las instalaciones de procesamiento de información.			
N.°	**Indicadores**	**Puntos**	**Observaciones**

145	La empresa cuenta con mínimo dos proveedores de redes e instalaciones de procesamiento de información crítica.	3	La empresa cuenta con dos proveedores.
146	Hace uso de redes redundantes.	3	
147	Cuenta con dos centros de datos separados geográficamente con sistemas duplicados.	3	La empresa cuenta únicamente con un centro de datos, el cual es suficiente para cumplir con la demanda.
148	Utiliza fuentes de alimentación físicas redundantes.	1	No, únicamente el ICE.
149	La carga automática se encuentra equilibrada entre ellas, mediante el uso de múltiples instancias paralelas de componentes de software.	3	
150	Se tiene componentes duplicados en sistemas o en redes.	3	Se cuenta con un servidor replica.

Promedio	3	**Nivel de cumplimiento:** Alto

Registro			
Objetivo: registrar eventos, generar evidencia, garantizar la integridad de la información de registro, prevenir el acceso no autorizado, identificar eventos de seguridad de la información que pueden conducir a un incidente de seguridad de la información y respaldar investigaciones.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
151	Se registran las identidades de los usuarios.	3	
152	Se registran las actividades que se realizan en el sistema.	3	Se registra en una bitácora lo que hace cada usuario.
153	Se guardan las fechas, horas y detalles de los eventos importantes.	3	

154	Se almacena la identidad del dispositivo usado, el identificador del sistema y la ubicación actual.	2	El identificador del dispositivo sí, la ubicación no.
155	Se registran las direcciones de red y protocolos involucrados.	3	
156	Se registran los intentos de acceso al sistema, tanto los que se realizaron de forma exitosa como los que se rechazaron.	3	Sí, por medio de *active directory*.
157	Los datos correctos, incorrectos y todo aquel intento de acceso a los recursos.	3	
158	Se registra los cambios en la configuración del sistema.	2	El usuario no puede realizar cambios.
159	El uso de privilegios es registrado.	3	
160	El uso de programas de utilidad y aplicaciones.	3	Todo queda en una bitácora.

161	Se registran los archivos a lo que se accede y su tipo de acceso, incluyendo la eliminación de datos importantes.	3	Solo se registra lo que se realiza en el sistema.
162	Las alarmas que se emiten por parte del sistema de control de acceso se registran.	2	Únicamente lo que se registra en el *active directory*.
163	Se guardan la activación y desactivación de sistemas de seguridad.	3	Queda un registro por parte del antivirus, con datos como dirección Mac, nombre etc. Todo se realiza con el Antivirus Eset EndPoint Security.
164	Registran la creación, modificación o suspensión de identidades.	1	No se guarda esa información.
165	Se registra las transacciones que el usuario ejecuta en las aplicaciones.	3	Los usuarios no utilizan aplicaciones,

			únicamente el sistema.
166	Existe una protección contra alteraciones en los tipos de mensajes registrados.	3	Se realiza mediante Eset End Pont Security.
167	Los archivos de registro que se editan o se eliminan se encuentran protegidos ante eventualidades.	3	Se monitorea toda la actividad por medio de un *dashboard* que brinda el antivirus.
168	Se cuenta con un plan en caso de fallar el registro de eventos o se sobrescriban eventos registrados en el pasado.	1	
169	Los expertos que realizan el análisis cuentan con las habilidades necesarias.	3	
170	Se cuenta con un procedimiento para el análisis de registros.	1	
171	Los atributos que requiere cada evento se encuentran relacionado con la seguridad.	1	

172	Se cuenta con una lista de excepciones identificadas previamente, mediante el uso de reglas predeterminadas.	1	No es necesario.
173	Se realizan análisis de patronos de comportamientos y tráfico de red estándar, comparándolos con actividad anómala y otros comportamientos.	3	Por medio del antivirus.
174	Se entrega un resultado del análisis de tendencias o patrones.	3	
175	Se realiza un análisis por medo de inteligencia de amenazas disponibles.	3	Por medio del antivirus Eset.
176	Se revisan los intentos exitosos y fallidos al acceder a recursos protegidos.	2	Únicamente por medio del *active directory.*
177	Se realiza una verificación de los registros de DNS, para la identificación de conexiones de red salientes a servidores maliciosos.	3	Sí, únicamente se cuenta con DNS para los servidores de la empresa, por lo tanto, se revisa desde ahí.

178	Se examinan los informes de uso de los proveedores de servicios.	1	
179	Se incluyen los registros de eventos de monitoreo físico.	1	
180	Se realiza una correlación de registros que permiten un análisis eficiente y muy preciso.	1	
Promedio		2	**Nivel de cumplimiento:** Medio

Actividades de seguimiento **Objetivo:** detectar comportamientos anómalos y posibles incidentes de seguridad de la información.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
181	Se monitorea el tráfico de red, sistema y aplicación tanto entrante como saliente.	3	Se monitorea el tiempo que se considere necesario.
182	Se da seguimiento a los accesos a los sistemas, servidores, equipos de red, sistemas de monitoreo y aplicaciones críticas.	2	Regularmente.
183	Los archivos de configuración de red y los sistemas de nivel crítico o administrativos cuentan con sistema de monitoreo.	3	
184	Monitorean los registros de herramientas de seguridad.	3	Se realiza por medio de Eset End Point Security.

185	Se monitorea los registros de eventos que se relacionan a la actividad del sistema y red.	3	
186	Se comprueba que el código que se ejecuta se encuentre autorizado y este no se haya manipulado.	3	Únicamente el personal de TI cuenta con acceso.
187	Se da seguimiento al uso de recursos y su rendimiento.	3	Por medio de monitoreo regular.
188	Se revisan la utilización de los sistemas en periodos normales y pico.	3	
189	Se revisa la hora habitual de acceso, ubicación y frecuencias de cada usuario o grupo.	3	
190	Se monitorea la terminación de procesos o aplicaciones no planificadas.	3	Se realiza por medio de Eset End Point Security.
191	Se observa la actividad típica asociada con el *malware* o tráfico que se origina en direcciones IP maliciosas conocidas.	3	Se monitorea por medio se Eset.

192	Se conocen las características de ataques más conocidos.	3	Únicamente ha habido un caso de *phishing*.
193	Se busca comportamientos inusuales del sistema.	3	Se monitorea por medio de Eset.
194	Se monitorea en búsqueda de comportamientos de cuellos de botella y sobrecargas.	3	Se asigna un ancho de banda a cada usuario.
195	Se tiene control sobre el acceso no autorizado a sistemas o información.	3	Se cuenta con una bitácora en la cual se registra la actividad de los usuarios.
196	Monitoreo para evitar escaneos no autorizados de aplicaciones comerciales, sistemas y redes.	3	Se realiza por medio de Eset End Point Security.
197	Se verifican los intentos exitosos y fallidos en accesos a los recursos protegidos.	1	
198	Búsqueda de comportamientos poco usuales del usuario y del sistema comparándolo con el resultado esperado.	2	Se monitorea en ocasiones, pero no

			se realiza una comparación.
Promedio		3	**Nivel de cumplimiento:** Alto
Instalación de software en sistemas operativos **Objetivo:** garantizar la integridad de los sistemas operativos y evitar la explotación de vulnerabilidades técnicas.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
199	Solo el personal autorizado realiza actualizaciones del software operativo.	3	Únicamente el personal de TI.
200	Se aseguran de que el código ejecutable previamente aprobado, sea el instalado y no otro código de desarrollo o compiladores en sistemas operativos.	3	Ya que únicamente el personal de TI realiza modificaciones.
201	Los softwares que se instalan pasaron por pruebas extensas y exitosas.	3	Es software de uso frecuente y se mantiene en un servidor.

202	Las bibliotecas fuente de programas se actualizan.	3	Actualizan de manera manual cuando es necesario.
203	Usan un sistema de inspección de configuración para mantener el control de todo el software operativo, incluso la documentación del sistema.	3	
204	Se tiene definida una estrategia de reversión antes de la implementación de cambios.	3	No, porque los cambios que se aplican son mínimos. Solamente en caso de actualizaciones.
205	Se cuenta con registros de auditoría de todas las actualizaciones del sistema operativo.	1	
206	Se archivan las versiones antiguas de software, con la información, parámetros requeridos, procedimientos, detalles de configuración y software de soporte como medida de contingencia y en caso de que	3	Sí, se mantienen archivadas en caso de que sea necesario revertir alguna actualización.

	sea necesario para leer o procesar datos archivados.		
Promedio		3	**Nivel de cumplimiento:** Alto
Seguridad de redes **Objetivo:** proteger la información en las redes y sus instalaciones de procesamiento de información de apoyo del compromiso a través de la red.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
207	Se cuenta con el tipo y nivel de clasificación de información que la red puede soportar.	3	
208	Se establecen responsabilidades y procedimientos para la gestión de equipos de red y dispositivos.	3	Únicamente el Departamento de Informática y el *outsourcing* que ayuda a la empresa con la parte de redes.

209	La documentación con los diagramas de red y archivos de configuración de los dispositivos se encuentra actualizada.	3	Se mantienen respaldados frecuentemente las configuraciones de los *switches* y *routers*.
210	Se tiene separada la responsabilidad operativa de las redes de las operaciones del sistema TIC cuando corresponda.	3	Solamente hay dos encargados de TI y ambos se encargan de la parte de redes, omitiendo al *outsourcing*.
211	Se tiene establecido controles para salvaguardar la confiabilidad e integridad de los datos que pasan a través de redes públicas, de terceros o redes inalámbricas, protegiendo también los sistemas conectados y las aplicaciones.	1	No cuentan con un tipo de control para estos casos.
212	Se tiene un registro y seguimiento adecuado para permitir la grabación y detección de acciones que pueden	1	

	afectar o son relevantes para la seguridad de la información.		
213	Se coordina estrechamente las actividades de gestión de la red, con el fin de optimizar el servicio a la organización, para la asegurar que se apliquen los controles consistentes en todo el proceso.	3	Al contar con dos proveedores, las redes están divididas, uno ve la parte local *wifi* y red, al haber varios servidores se utiliza una red aislada, el área de bodegas está aislada del área administrativa, porque se cuenta con red hasta el final de la bodega.
214	Se tiene sistemas de autenticación en la red.	3	
215	Se restringen y filtran las conexiones de los sistemas a la red.	3	Todos los dispositivos cuentan

			con distintas contraseñas.
216	Se detecta, restringen y autentican la conexión de equipos y dispositivos a la red.	3	Se utiliza una herramienta llamada Winbox para monitorear toda la actividad de red.
217	Se endurecen los dispositivos de red.	3	Sí, se utiliza seguridad en todos los dispositivos.
218	Se segregan los canales de administración de red de otro tráfico de red.	3	
218	Se aíslan de manera temporal las subredes críticas, si esta se encuentra bajo ataque.	3	Nunca ha habido un ataque y en caso de haberlo sería controlable, porque todas las zonas se encuentran separadas para el

			caso de que llegue a haber un ataque.
219	Se deshabilitan protocolos de red vulnerables.	3	
Promedio		3	**Nivel de cumplimiento:** Alto

Seguridad de los servicios de red **Objetivo:** garantizar la seguridad en el uso de los servicios de red.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
220	Se puede acceder a las redes y los servicios de red.	3	
221	Existen requisitos de autenticación para acceder a diversos servicios de red.	1	Pero no es el adecuado, el personal considera que no cuentan con los mejores requisitos.

222	Hay procedimientos de autorización para determinar a quién se le permite acceder a qué redes y en qué red de servicio.	1	Es un tema muy al azar, pero no queda documentado. En ocasiones se duplican perfiles para asignarlos a personas con cargos similares.
223	Se tiene gestión de la red, controles y procedimientos tecnológicos para proteger el acceso a la red, conexiones y servicios de red.	1	Se cuenta con herramientas para dominio, pero todo es a criterio del personal de TI, es decir, no cuentan con procedimientos.
224	Existe medios utilizados para acceder a redes y servicios de red.	3	Se utilizan herramientas, Wifi, VPN, etc.
225	Se tiene implementado el registro de hora, ubicación y otros atributos del usuario al momento del acceso.	1	

226	Hay seguimiento del uso de los servicios de red.	3	No están pendientes, pero sí existe la herramienta.
227	Existen servicios para seguridad de red, como autenticación, encriptación y controles de conexión de red	3	Autentificación de Windows, VPN, Wifi, etc.
228	Hay parámetros técnicos para la conexión segura con los servicios de red, de acuerdo con las normas de seguridad y conexión a la red.	1	Existen herramientas, consultoría, pero no existen procedimientos o políticas que indiquen dichos parámetros.
229	Hay almacenamiento en caché de acuerdo con los requisitos de rendimiento, disponibilidad y confidencialidad.	1	
230	Hay procedimientos para el uso de servicios de red para restringir el acceso a servicios o aplicaciones de red.	1	No existen procedimientos documentados.

Promedio		2	**Nivel de cumplimiento:** Medio
Segregación de redes **Objetivo:** dividir la red en límites de seguridad y controlar el tráfico entre ellos en función de las necesidades comerciales			
N.°	**Indicadores**	**Puntos**	**Observaciones**
231	Hay gestión de la seguridad de las grandes redes, dividiéndolas en dominios separados de red y también de la red pública.	3	Existen dos dominios con reglas diferentes, a nivel de *wifi* existe una segregación para cada zona de la empresa. Se cuenta con una red separada para comunicar las sucursales.
232	Se puede elegir en función de los niveles de confianza, criticidad y sensibilidad de los dominios.	3	

232	Se usan redes físicamente diferentes o usando diferentes redes lógicas.	3	En el caso de zonas y sucursales se utilizan redes separadas que cuentan con su respectivo nivel de seguridad.
233	Están bien definidos los perímetros de cada dominio.	2	Sí, pero parcialmente, el personal considera que se puede mejorar. Ya que es posible visualizar direcciones IP que no deberían poder verse.
234	Se permite el acceso entre dominios de red, debe controlarse en el perímetro mediante una puerta de enlace.	3	
235	Cuenta con la política específica del tema sobre control de acceso, requisitos de acceso, valor y clasificación de la información procesada.	1	No existen políticas en la empresa.

236	Tiene en cuenta el costo relativo y el impacto en el rendimiento de incorporar tecnología de puerta de enlace adecuada.	1	
Promedio		3	**Nivel de cumplimiento:** Alto
Filtrado web **Objetivo:** proteger los sistemas contra el malware y evitar el acceso a sitios web no autorizados.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
237	Los sitios web a los que se accede, cuentan con función de carga de información, están permitidos por razones comerciales válidas.	1	No se ha realizado.
238	Existe acceso a sitios web maliciosos conocidos o sospechosos.	1	
239	Hay servidores de mando y control.	1	Si existe el *firewall*, pero no está configurado.

240	Se encuentran sitios web maliciosos adquiridos de inteligencia de amenazas.	1	
241	Se encontraron sitios web que comparten contenido ilegal.	1	
Promedio		1	**Nivel de cumplimiento:** Bajo

Separación de los entornos de desarrollo, prueba y producción **Objetivo:** proteger el entorno de producción y los datos contra el compromiso de las actividades de desarrollo y prueba.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
253	Se separan adecuadamente los sistemas de desarrollo y producción y operarlos en distintos dominios.	1	
254	Se definen, documentan e implementan reglas y autorizaciones para el despliegue de software del estado de desarrollo al estado de producción.	1	Se hace por parte del proveedor.

255	Se prueban los cambios en los sistemas de producción y aplicaciones en un entorno de pruebas o etapas antes de aplicarse a dichos sistemas.	1	Se hace por parte del proveedor.
256	Se han probado los sistemas en ambientes de producción excepto en circunstancias que han sido definidas y aprobadas.	1	
257	Se usan herramientas de desarrollo o programas de utilidad que no sean accesibles desde sistemas de producción cuando no se requiera.	1	
258	Se muestran etiquetas de identificación del entorno, adecuadas en los menús para reducir el riesgo de error.	1	
259	Se copia información confidencial en los entornos del sistema de desarrollo y prueba, a menos que se proporcionen controles equivalentes para los sistemas de desarrollo y prueba.	1	

260	Se aplican parches y actualizaciones a todas las herramientas de desarrollo, integración y prueba.	1	
261	Existe una configuración segura de sistemas y software.	3	
262	Se tiene control de acceso a los ambientes.	3	
263	Hay seguimiento de cambios en el entorno y código almacenado en el mismo.	3	
264	Se monitorea para asegurar los ambientes.	3	Parcialmente.
265	Realización de copias de seguridad de los entornos.	3	De servidores en discos protegidos y en algunos casos en unidades extraíbles.

Promedio	2	**Nivel de cumplimiento:** Medio

Gestión de cambios **Objetivo:** preservar la seguridad de la información al ejecutar cambios.			
N.°	**Indicadores**	**Puntos**	**Observaciones**
266	Hay planificación y evaluación del impacto potencial de los cambios, considerando todas las dependencias.	1	Por un tema de cultura, primero se cambia y después se piensa en lo que viene.
267	Existen autorizaciones a cambios.	3	
268	Se comunican los cambios a las partes interesadas relevantes.	3	
269	Se realizan pruebas y aceptación de pruebas para los cambios.	3	No en todos los casos.
270	Se implementan cambios, incluidos los planes de implementación	1	
271	Se toman consideraciones de emergencia y contingencia, incluidos los procedimientos de respaldo	1	No existen procedimientos

			en caso de emergencia.
272	Almacenan registros de cambios que incluyan todo lo anterior	1	
273	Aseguran que la documentación operativa y los procedimientos del usuario se cambien según sea necesario	1	No existen procedimientos.
274	Garantizan que se cambien los planes de continuidad de las TIC y los procedimientos de respuesta y recuperación	1	No existen procedimientos.
Promedio		2	**Nivel de cumplimiento:** Medio

Anexo 7: Políticas de seguridad físicas Distribuidora COARSA

POLÍTICAS DE SEGURIDAD FÍSICA

NORMA ISO 27002:2022

DPTO. INFORMÁTICA

Código: 07.3-MP-01

Versión 1.0

San Ramón, Costa Rica

Mayo, 2023

CONTENIDO

SIGLAS, ABREVIATURAS Y CONCEPTOS

WETRANSFER: aplicación basada en la transferencia de archivos especialmente pesados, por medio de la nube.

DROPBOX: herramienta que permite sincronizar archivos a través de un directorio virtual o disco duro virtual de la red.

GOOGLE DRIVE: servicio de alojamiento de archivos.

FTP: (File Transfer Protocol) es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red.

RESUMEN

El propósito de este documento es ofrecer a la organización una guía detallada basada en la Norma ISO 27002:2022 que establece una serie de políticas de controles físicos de la seguridad de la información. El objetivo principal es fortalecer la ciberseguridad de la empresa, dado que en los últimos años se ha vuelto un factor crítico, debido al constante aumento de los ataques cibernéticos. La presente guía incluye un total de 13 controles cuidadosamente seleccionados por el grupo de investigadores en colaboración con los responsables de Tecnologías de la Información de la Organización. Estos controles se consideran fundamentales para mitigar los riesgos asociados con la seguridad física de los activos de información. La aplicación de estos controles físicos permitirá a la Organización proteger sus recursos de información y salvaguardar la confidencialidad, integridad y disponibilidad de los datos críticos. Los controles propuestos abarcan aspectos clave como la seguridad de las instalaciones, la protección de los equipos y dispositivos, el control de acceso, la gestión de visitantes y la supervisión de las áreas restringidas. Cada uno de los controles se ha diseñado para adaptarse a las necesidades específicas de la Organización y cumplir con los requisitos de la Norma ISO 27002:2022. Al seguir estas políticas de controles físicos, la organización podrá fortalecer su postura de seguridad cibernética y reducir la probabilidad de sufrir incidentes relacionados con la seguridad de la información. Asimismo, se promoverá una cultura de seguridad en toda la empresa, involucrando a todos los empleados

en la protección activa de los activos de información y en la prevención de posibles brechas de seguridad.

INTRODUCCIÓN

La ciberseguridad representa en la actualidad una preocupación esencial para las empresas, debido al constante incremento de los ataques cibernéticos. Con el objetivo de abordar este desafío y salvaguardar los activos de información de una organización, se presenta este documento que ofrece una detallada guía basada en la Norma ISO 27002:2022.

OBJETIVO

El propósito de este documento es proporcionar a la organización una completa guía basada en la Norma ISO 27002:2022, que establece políticas de controles físicos. Su principal objetivo es fortalecer la ciberseguridad de la empresa frente al creciente número de ataques cibernéticos. A través de la implementación de estos controles, se busca mitigar los riesgos asociados con la seguridad física de los activos de información, proteger los recursos de información y garantizar la confidencialidad, integridad y disponibilidad de los datos críticos.

ALCANCE

Este documento abarca la definición y descripción de un total de 13 controles físicos, cuidadosamente seleccionados por los creadores de este documento y los responsables de Tecnologías de la Información de la Organización. Estos controles

abordan aspectos clave como la seguridad de las instalaciones, la protección de los equipos y dispositivos, el control de acceso, la gestión de visitantes y la supervisión de las áreas restringidas, entre otros.

MARCO DE REFERENCIA

Este documento se basa en la Norma ISO 27002:2022, la cual establece los requisitos para el establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información. Los controles físicos propuestos en este documento se alinean con los principios y buenas prácticas establecidos en esta Norma, con el fin de garantizar que la organización cumpla con los estándares internacionales y las mejores prácticas en materia de seguridad de la información.

Además, se toma en consideración las necesidades específicas de la organización y se ha diseñado para adaptarse a su entorno y características particulares. Al seguir las políticas de controles físicos aquí descritas, la organización fortalecerá su postura de seguridad cibernética, reduciendo la probabilidad de sufrir incidentes relacionados con la seguridad de la información. También se fomentará una cultura de seguridad en toda la empresa, involucrando a todos los empleados en la protección activa de los activos de información y en la prevención de posibles brechas de seguridad.

Políticas de seguridad de la información: controles físicos

1.Perímetros de seguridad física

Objetivo

Evitar el acceso físico no autorizado, el daño y la interferencia a la información de la organización y otros activos asociados.

1.1 Perímetros sólidos

a) Todos los edificios que contengan instalaciones de procesamiento de información deben contar con perímetros físicamente sólidos, sin espacios o áreas donde un robo pueda ocurrir fácilmente.
b) Se deben tomar medidas adicionales para asegurar las zonas como la recepción, abiertas y que representan un mayor riesgo de acceso no autorizado.
c) Se debe implementar medidas de seguridad visibles en todas las áreas de la Organización, incluyendo escritorios de uso público.

1.2 Construcción sólida

a) Los techos, paredes y pisos de las instalaciones de la empresa deben ser de construcción sólida para evitar intrusiones físicas no autorizadas.
b) Se deben realizar inspecciones regulares para verificar la integridad de la estructura y tomar medidas correctivas en caso de detección de vulnerabilidades.

1.3 Protección de puertas y ventanas

a) Todas las puertas exteriores y ventanas deben contar con mecanismos de control adecuados para protegerlas contra el acceso no autorizado, como rejas, alarmas y cerraduras seguras.
b) Se debe revisar y mantener regularmente los sistemas de seguridad instalados en puertas y ventanas para asegurar su correcto funcionamiento y detección de posibles fallas.

1.4 Revisión de puertas contra incendios

a) Las puertas contra incendios deben revisarse constantemente por el personal a cargo, para garantizar que estén en buen estado y funcionamiento.
b) Se debe designar una brigada responsable de realizar estas revisiones y llevar un registro de las inspecciones realizadas, así como de cualquier acción correctiva necesaria.

2.Entrada Física

Objetivo

Garantizar solo el acceso físico autorizado a la información de la organización y otros activos asociados.

2.1 Acceso permitido solo al personal autorizado

a) El acceso a los sitios y edificios debe estar restringido únicamente al personal autorizado.

b) Se deben implementar medidas de control en la entrada, como solicitar datos personales al guarda de seguridad y emitir gafetes de identificación a todos los funcionarios.

2.2 Registro de auditoría de accesos

a) El personal encargado de las áreas donde se procesa información confidencial debe contar con un libro o registro físico o electrónico de auditoría en el cual se registren todos los accesos.
b) Se deben mantener registros precisos y actualizados de los accesos a estas áreas, lo cual contribuye a la trazabilidad y la responsabilidad.

2.3 Mecanismos técnicos de gestión de acceso

a) Debe haber mecanismos técnicos para gestionar el acceso a las áreas donde se procesa o almacena información, como tarjetas de acceso, biometría o autenticación de dos factores.
b) Se debe asegurar que todos los funcionarios cuenten con el medio de acceso adecuado para ingresar a las áreas pertinentes.

2.4 Área de recepción supervisada

a) Se debe establecer un área de recepción supervisada por personal u otros medios para controlar el acceso físico al sitio o edificio.
b) El personal de seguridad en la entrada del edificio debe ser responsable de supervisar y controlar el acceso de las personas.

2.5 Inspección de pertenencias

a) El personal de seguridad debe inspeccionar las pertenencias de los funcionarios y personas externas al ingresar o salir de las instalaciones.
b) Se deben realizar inspecciones adecuada y consistentemente para detectar posibles amenazas o riesgos de seguridad.

2.6 Identificación visible

a) Tanto el personal como las partes interesadas deben utilizar algún tipo de identificación visible, como gafetes o insignias que los distinga como empleados permanentes, proveedores o visitantes.
b) Se debe fomentar el uso correcto y visible de la identificación para facilitar la identificación de las personas en las instalaciones.

2.7 Acceso a zonas restringidas

a) El acceso a zonas restringidas debe otorgarse únicamente a personas externas a la empresa en casos estrictamente necesarios.
b) Se deben establecer procedimientos claros y controles adicionales para garantizar que solo se permita el acceso necesario y autorizado a estas áreas.

2.8 Áreas de carga y descarga

a) Las áreas de carga y descarga deben estar diseñadas de manera que las entregas se realicen sin que el personal de entrega obtenga acceso no autorizado a otras partes del edificio.
b) Se debe contar con la supervisión adecuada para prevenir situaciones de riesgo y asegurar la integridad de las áreas restringidas.

2.9 Inspección de entregas

a) Se debe inspeccionar y examinar las entregas entrantes en busca de explosivos, productos químicos u otros materiales peligrosos antes de que se muevan de las áreas de entrega y carga.
b) Es fundamental implementar procedimientos de inspección para mitigar posibles riesgos asociados a las entregas recibidas.

2.10 Separación y verificación de envíos

a) Se deben separar físicamente tanto los envíos entrantes como los salientes y se deben inspeccionar las entregas que ingresan en busca de evidencia de manipulación en el camino.
b) Se deben realizar verificaciones periódicas por parte de distintos funcionarios para garantizar la integridad de los envíos y detectar posibles manipulaciones o irregularidades.

3.Seguridad de oficinas, salas e instalaciones

Objetivo

Prevenir el acceso físico no autorizado, el daño y la interferencia a la información de la organización y otros activos asociados en las oficinas, salas e instalaciones.

3.1 Ubicación de oficinas de acceso restringido

a) Las oficinas designadas como de acceso restringido deben estar ubicadas en lugares de difícil acceso para el público en general.
b) Las zonas críticas, como el centro de datos y la zona de chequeo de mercadería deben estar estratégicamente ubicadas en áreas consideradas seguras.
c) Se debe evaluar la necesidad de mejorar la seguridad de la puerta del centro de datos, considerando que, aunque está ubicado en una zona segura con llave, su puerta de cristal transparente permite cierta visibilidad parcial.

3.2 Discreción en zonas de procesamiento de información

a) Las zonas donde se procesa información confidencial deben ser discretas y no deben contar con señalización que indique el tipo de actividad que se realiza.
b) Se deben implementar medidas para evitar cualquier forma de señalización visible que pueda comprometer la confidencialidad y la seguridad de la información en las zonas críticas.

3.3 Privacidad en las instalaciones

a) Las instalaciones de la empresa deben brindar privacidad suficiente para garantizar que las actividades privadas no sean visibles ni audibles desde el exterior.
b) Se debe evaluar la necesidad de implementar medidas adicionales para proteger la privacidad en áreas donde existan paredes de vidrio transparentes.
c) Se deben tomar medidas para garantizar que las conversaciones dentro de las instalaciones sean indistintas y no puedan escucharse fuera de las áreas autorizadas.

3.4 Confidencialidad de guías telefónicas y mapas

a) Las guías telefónicas y mapas de zonas de la empresa deben ser considerados confidenciales y no deben estar disponibles para cualquier persona.
b) Se debe establecer controles y restricciones para garantizar que solo las personas autorizadas tengan acceso a estas herramientas.
c) Es importante asegurar que la divulgación indiscriminada de guías telefónicas y mapas no comprometa la confidencialidad y seguridad de la información.

4. Protección contra Amenazas Físicas y Ambientales

Objetivo

Prevenir o reducir las consecuencias de eventos originados por amenazas físicas y ambientales.

4.1 Consideraciones topográficas y de construcción

a) Al ubicar y construir las instalaciones, se debe tener en cuenta la topografía local, como la elevación adecuada, la presencia de masas de agua, las fallas tectónicas y las amenazas urbanas.
b) Se debe tomar medidas para mitigar los riesgos asociados con estas amenazas, asegurando que las instalaciones estén ubicadas y construidas de manera que reduzcan las posibles consecuencias de eventos físicos y ambientales.

4.2 Detección temprana de incendios e inundaciones

a) La empresa debe contar con sistemas capaces de detectar incendios o inundaciones en una etapa temprana.
b) Estos sistemas deben estar diseñados para evitar que el fuego o el agua dañen los medios de almacenamiento y los dispositivos relacionados, como los sistemas de procesamiento de información.

c) Se debe establecer un plan adecuado de respuesta y contingencia en caso de detección de incendios o inundaciones.

4.3 Protección contra sobretensiones eléctricas

a) La empresa debe contar con sistemas capaces de proteger los sistemas de información, tanto del servidor como del cliente, contra sobretensiones eléctricas u otros eventos similares.
b) Estos sistemas de protección deben implementarse para minimizar las consecuencias de tales eventos y preservar la integridad de los sistemas de información.

4.4 Inspecciones aleatorias de seguridad

a) Se deben llevar a cabo inspecciones aleatorias para detectar explosivos o armas en el personal, vehículos o mercancías que ingresan a las instalaciones de procesamiento de información confidencial.
b) Estas inspecciones deben realizarse tanto al entrar como al salir de la empresa y también deben aplicarse a la entrada y salida de mercadería.
c) Se deben establecer procedimientos claros y controles adecuados para garantizar la seguridad de las instalaciones y prevenir posibles amenazas físicas.

5.Trabajar en Áreas Seguras

Objetivo

Proteger la información y otros activos asociados en áreas seguras contra daños e interferencias no autorizadas por parte del personal que trabaja en estas áreas.

5.1 Divulgación Selectiva

a) El personal solo debe informarse sobre las actividades en áreas seguras cuando sea absolutamente necesario.

b) Se establecerán procesos para garantizar que la información relevante se comunique selectiva y controladamente, evitando divulgaciones innecesarias.

5.2 Supervisión en Áreas Seguras

a) Se prohíbe el trabajo sin supervisión en áreas seguras, con el fin de salvaguardar la seguridad y reducir el riesgo de actividades maliciosas.

b) Todas las áreas seguras deben estar protegidas mediante sistemas de cierre y control de acceso, como cerraduras y llaves.

5.3 Inspecciones en Áreas Seguras Vacantes

a) Se llevarán a cabo inspecciones periódicas en áreas seguras que se encuentren desocupadas.

b) Estas inspecciones tienen como objetivo asegurar que las áreas seguras no sean utilizadas sin autorización y tomar las medidas necesarias para su protección.

5.4 Restricción de Equipos de Grabación

a) Se prohíbe el uso de equipos fotográficos, de video, de audio y otros dispositivos de grabación en áreas seguras.
b) Esta restricción tiene como finalidad prevenir la divulgación no autorizada de información confidencial y preservar la privacidad de las actividades en dichas áreas.

5.5 Control de Dispositivos Terminales

a) Se implementarán medidas para controlar adecuadamente el transporte y uso de dispositivos terminales por parte del personal en áreas seguras.

b) Se establecerán procedimientos y controles para garantizar el cumplimiento de las políticas de seguridad relacionadas con estos dispositivos.

5.6 Acceso a Procedimientos de Emergencia

a) Los procedimientos de emergencia relacionados con áreas seguras estarán disponibles de manera visible y accesible.

b) Se asegurará que el personal esté informado sobre estos procedimientos para una respuesta efectiva en situaciones de emergencia.

6. Escritorio y Pantalla Despejados

Objetivo

Reducir los riesgos de acceso no autorizado, pérdida y daño de la información en escritorios, pantallas y en otros lugares accesibles durante y fuera del horario normal de trabajo.

6.1 Protección de Información Confidencial en Escritorios

a) Se debe proteger la información comercial confidencial o crítica cuando no sea requerida, especialmente durante períodos de ausencia del personal o cuando un cargo quede vacante.

b) Se establecerán procedimientos para garantizar que la información se guarde de manera segura, como en archivos cerrados con llave o mediante otras medidas de protección física.

6.2 Protección de Dispositivos de Punto Final

a) Los dispositivos de punto final del usuario deben estar protegidos mediante cerraduras con llave u otros medios de seguridad cuando no están en uso.

b) Se promoverá el uso de mecanismos de bloqueo de pantalla para dispositivos desatendidos, asegurando que los datos y la información permanezcan protegidos.

6.3 Autenticación en Impresoras

a) Las impresoras deben contar con una función de autenticación para que solo los creadores de los documentos puedan obtener sus impresiones.

b) Se implementarán medidas para garantizar que los usuarios ingresen un código único o autenticación para acceder a las impresiones.

6.4 Almacenamiento Seguro de Documentos y Medios Extraíbles

a) Los documentos y medios de almacenamiento extraíbles que contienen información confidencial deben almacenarse de manera segura.

b) Se establecerán procedimientos para el almacenamiento bajo llave de estos elementos cuando ya no sean necesarios.

6.5 Configuración de Ventanas Emergentes

a) Se establecerán reglas y orientación para la configuración de ventanas emergentes en las pantallas, como desactivar las nuevas

ventanas emergentes de correo electrónico y mensajería durante presentaciones, pantallas compartidas o en áreas públicas.

b) Se promoverá el uso de configuraciones apropiadas en los dispositivos y sistemas para minimizar el riesgo de exposición de información sensible.

6.6 Eliminación de Información en Pizarras y Pantallas

a) Se debe garantizar que la información sensible o crítica en pizarras y otros tipos de pantallas se borre cuando ya no sea necesaria.

b) Se fomentará el uso de medios seguros para la eliminación de datos en las pantallas.

7.Ubicación y protección del equipo

Objetivo

Reducir los riesgos de amenazas físicas y ambientales, y de accesos y daños no autorizados.

7.1 Acceso Restringido

a) La ubicación de los equipos evita el acceso innecesario a las áreas de trabajo, asegurando que solo el personal autorizado tenga acceso a ellos.

b) Se establecerán medidas de seguridad, como sistemas de cerraduras, tarjetas de acceso o biometría, para garantizar la protección contra accesos no autorizados.

7.2 Privacidad de Datos Confidenciales

a) Las instalaciones de procesamiento de información que manejan datos confidenciales se ubicarán estratégicamente para reducir el riesgo de que la información sea vista por personas no autorizadas durante su uso.

b) Se implementarán medidas de control, como paredes, puertas con cerradura y divisores de pantalla, para garantizar la privacidad de la información confidencial.

7.3 Protección contra Amenazas Físicas y Ambientales

a) Se establecerán controles para minimizar el riesgo de posibles amenazas físicas y ambientales, como robo, incendio, explosivos, humo, agua, fallas en suministros, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo.

b) Se designará una brigada de seguridad encargada de rotular las zonas y tomar medidas para minimizar los riesgos.

7.4 Comportamiento en las Instalaciones

a) Se establecerán reglas para comer, beber y fumar en la cercanía de las instalaciones de procesamiento de información para evitar riesgos y proteger los equipos y la seguridad en general.

7.5 Monitoreo Ambiental

a) Se realizará una constante monitorización de las condiciones ambientales, como temperatura y humedad, en busca de condiciones que puedan afectar negativamente el funcionamiento de las instalaciones de procesamiento de información.

b) Se implementarán sistemas de control y alarmas para detectar y notificar desviaciones de las condiciones ambientales aceptables.

7.6 Protección contra Rayos

a) Se aplicará protección contra rayos a todos los edificios y se colocarán filtros de protección contra rayos en todas las entradas de líneas eléctricas y de comunicaciones.

b) Se realizarán inspecciones y mantenimientos periódicos para garantizar la efectividad de las medidas de protección contra rayos.

7.7 Protección de Equipos en Ambientes Industriales

a) Los equipos en ambientes industriales estarán protegidos con métodos especiales, como membranas de teclado, para garantizar su funcionamiento seguro y evitar daños causados por el entorno.

7.8 Protección contra Emanación Electromagnética

a) Se implementarán medidas de protección para los equipos que procesan información confidencial, a fin de minimizar el riesgo de fuga de información, debido a la emanación electromagnética.

7.9 Separación Física de Instalaciones

a) Las instalaciones de procesamiento de información gestionadas por la organización se separarán físicamente de aquellas no gestionadas por la organización.

b) Se implementarán medidas de seguridad, como cercas, puertas con cerradura.

8. Seguridad de los activos fuera de las instalaciones

Objetivo

Evitar la pérdida, el daño, el robo o el compromiso de los dispositivos externos y la interrupción de las operaciones de la organización.

8.1 Custodia Responsable de Dispositivos Externos

a) Los empleados deben ser responsables de mantener sus dispositivos externos bajo su control directo en todo momento.

b) Cuando no estén en uso, los dispositivos deben ser almacenados en lugares seguros, como cajones con llave o armarios de seguridad designados.

c) Los dispositivos externos no deben ser dejados desatendidos en ningún lugar público o visible en vehículos estacionados.

8.2 Autenticación y Acceso a Dispositivos Externos

a) Se debe implementar un proceso de autenticación sólido para acceder a los dispositivos externos, incluyendo contraseñas seguras, autenticación biométrica o tarjetas inteligentes.

b) Los dispositivos externos deben tener configurada la función de bloqueo automático después de un período breve de inactividad y requerir autenticación nuevamente para desbloquearlos.

c) En caso de pérdida o robo, los dispositivos deben tener la capacidad de ser bloqueados o deshabilitados de manera remota para prevenir el acceso no autorizado.

8.3 Respaldo y Almacenamiento Seguro

a) Los datos almacenados en dispositivos externos deben ser cifrados de manera obligatoria para proteger su confidencialidad en caso de pérdida o robo.

b) Se debe promover activamente el uso de servicios en la nube o servidores internos para respaldar y almacenar datos críticos, reduciendo la dependencia de los dispositivos externos como única fuente de almacenamiento.

c) Los empleados deben recibir capacitación sobre cómo realizar copias de seguridad de manera segura y cómo restaurar datos desde almacenamiento externo en caso necesario.

8.4 Protección contra Riesgos Ambientales

a) Se deben establecer pautas para proteger los dispositivos externos de condiciones ambientales extremas, como temperaturas excesivas, humedad o frío.

b) Los empleados deben tomar medidas para evitar situaciones que puedan dañar físicamente los dispositivos, como mantenerlos alejados de áreas de alto tráfico o asegurarlos en entornos con vibraciones o impactos frecuentes.

c) Se deben implementar medidas de protección para prevenir daños causados por eventos imprevistos, como derrames de líquidos o golpes accidentales.

8.5 Transporte Seguro de Dispositivos Externos

a) Los empleados deben utilizar fundas o estuches de protección duraderos para los dispositivos externos durante el transporte.

b) Los dispositivos externos nunca deben dejarse visibles en vehículos estacionados; deben ser guardados en lugares no visibles o en el maletero.

c) Durante el transporte, los dispositivos externos deben mantenerse cerca y bajo el control directo del propietario en todo momento.

8.6 Eliminación Segura de Dispositivos Externos

a) Antes de deshacerse de los dispositivos externos, se debe realizar un proceso de desactivación que incluya la eliminación de datos personales y la restauración a la configuración de fábrica.

b) Los dispositivos deben ser sometidos a un proceso de eliminación seguro que incluya el borrado completo y permanente de datos almacenados, preferiblemente utilizando métodos de eliminación certificados.

c) La eliminación final de los dispositivos debe cumplir con las regulaciones ambientales y de seguridad de residuos electrónicos, ya sea a través de reciclaje autorizado o desecho adecuado.

9. Medios de Almacenamiento

Objetivo

Garantizar exclusivamente la autorización para divulgar, modificar, eliminar o destruir información almacenada, mediante la implementación de directrices y prácticas sólidas para el uso, acceso y transporte de medios de almacenamiento.

9.1 Establecimiento de Procedimientos para el Uso Adecuado de Medios de Almacenamiento

a) Se deberán establecer y difundir procedimientos claros y detallados que regulen el correcto uso de diversos tipos de medios de almacenamiento. Esto abarca desde discos duros externos hasta unidades USB y CD/DVD.

b) Se instruirá a los empleados acerca de cómo formatear y preparar los medios de almacenamiento antes de su uso, con el propósito de asegurar su adecuado funcionamiento y su integridad.

c) Las políticas incluirán pautas para el etiquetado adecuado de los medios de almacenamiento, con información identificativa y niveles de confidencialidad.

9.2 Aprobación y Autorización para el Uso de Medios de Almacenamiento Externos

a) Se requerirá la aprobación previa de la alta dirección o una autoridad designada antes de utilizar cualquier medio de almacenamiento externo que contenga información crítica, confidencial o sensible.

b) Se establecerá un proceso formal de autorización que incluirá la presentación de justificaciones fundamentadas para el uso del medio de almacenamiento y la identificación de un responsable claramente designado.

c) Se mantendrá un registro detallado de todas las aprobaciones y autorizaciones otorgadas para el uso de medios de almacenamiento externos.

9.3 Implementación de Cifrado de Datos en Medios de Almacenamiento Portátiles

a) Se exigirá que cualquier medio de almacenamiento portátil empleado para el transporte de información sensible cuente con cifrado de datos.

b) Los estándares de cifrados certificados serán implementados rigurosamente para garantizar la confidencialidad de la información durante su almacenamiento y transporte.

c) Se brindará capacitación a los empleados, de manera que estén familiarizados con la correcta habilitación y uso del cifrado en los medios de almacenamiento portátiles.

9.4 Control y Monitoreo del Uso de Medios de Almacenamiento

a) Se implementará un proceso continuo de seguimiento y registro exhaustivo, abarcando la asignación, el uso y el retorno de medios de almacenamiento tanto internos como externos.

b) Sistemas de gestión de inventario serán establecidos para asegurar un seguimiento preciso de la ubicación y estado de los medios de almacenamiento en todo momento.

c) Auditorías regulares serán efectuadas con el propósito de verificar el cumplimiento de las políticas establecidas y detectar posibles desviaciones en el uso de medios de almacenamiento.

9.5 Destrucción Segura de Medios de Almacenamiento Obsoletos

a) Se desarrollarán procedimientos meticulosos para la eliminación y destrucción segura de medios de almacenamiento que hayan quedado obsoletos o cuyo uso ya no sea requerido.

b) Métodos certificados de destrucción serán rigurosamente aplicados, tales como trituración o borrado seguro, con el fin de asegurar la completa y permanente eliminación de la información contenida en dichos medios.

c) Se mantendrán registros detallados de todos los procesos de destrucción, incluyendo fechas, métodos implementados y responsables involucrados en dichos procedimientos.

10. Utilidades de apoyo

Objetivo

Evitar la pérdida, el daño o el compromiso de la información y otros activos asociados, o la interrupción de las operaciones de la organización debido a fallas e interrupciones de los servicios públicos de apoyo.

10.1 Establecimiento de Procedimientos para la Administración de Utilidades de Apoyo

a) Se establecerán procedimientos detallados para la administración eficaz de las utilidades de apoyo, que incluyen electricidad, agua, comunicaciones y otros servicios esenciales.

b) Se definirán responsabilidades claras para monitorear y garantizar el suministro continuo y confiable de las utilidades de apoyo.

c) Se implementará un sistema de alerta temprana y respuesta para detectar y abordar posibles fallas o interrupciones en los servicios públicos de apoyo.

10.2 Respaldo y Planificación de Continuidad en Caso de Interrupciones de Utilidades

a) Se establecerá un plan de respaldo detallado para asegurar el suministro alternativo de utilidades en caso de interrupciones prolongadas.

b) Se identificarán recursos y proveedores alternativos de utilidades para garantizar la continuidad de las operaciones en situaciones de emergencia.

c) Se realizarán simulacros regulares de interrupciones de utilidades para probar la efectividad del plan de continuidad y realizar mejoras necesarias.

10.3 Mantenimiento Preventivo y Correctivo de Infraestructuras de Utilidades

a) Se implementará un programa de mantenimiento preventivo regular para asegurar el funcionamiento óptimo y confiable de las infraestructuras de utilidades.

b) Los equipos de mantenimiento deberán estar capacitados y equipados adecuadamente para abordar tanto problemas preventivos como correctivos.

c) Se llevarán registros detallados de todas las actividades de mantenimiento realizadas, incluyendo fechas, descripciones y resultados.

10.4 Monitoreo Continuo y Gestión de Riesgos Relacionados con Utilidades

a) Se establecerán sistemas de monitoreo constante para detectar anomalías en el suministro de utilidades y tomar medidas preventivas de inmediato.

b) Se evaluarán y gestionarán los riesgos asociados con las interrupciones de utilidades, identificando medidas de mitigación y planes de respuesta.

c) Los informes periódicos de gestión de riesgos se presentarán a la alta dirección para garantizar la toma de decisiones informadas.

10.5 Capacitación y Concientización del Personal con Relación a Utilidades de Apoyo

a) Se brindará capacitación regular a los empleados sobre la importancia de las utilidades de apoyo y su papel en la continuidad operativa.

b) Se promoverá la conciencia sobre prácticas de uso eficiente de utilidades para minimizar el impacto ambiental y reducir costos operativos.

c) Los empleados recibirán instrucciones claras sobre cómo informar y abordar problemas relacionados con las utilidades de apoyo de manera oportuna.

11. Seguridad del cableado

Objetivo

Evitar la pérdida, el daño, el robo o el compromiso de la información otros activos asociados y la interrupción de las operaciones de la organización relacionadas con el cableado de energía y comunicaciones.

11.1 Implementación de Estándares de Cableado Seguro

a) Se establecerán y promoverán estándares de cableado seguro para garantizar una instalación ordenada y confiable de cables de energía y comunicaciones.

b) Se proporcionarán pautas claras sobre cómo realizar la organización y gestión adecuada de los cables para minimizar riesgos y asegurar un acceso eficiente.

11.2 Seguridad Física de las Infraestructuras de Cableado

a) Se tomarán medidas para proteger las infraestructuras de cableado contra acceso no autorizado, daños intencionales o accidentales y robos.

b) Se implementarán restricciones de acceso físico a las áreas de cableado para asegurar que solo personal autorizado tenga permitido ingresar.

11.3 Mantenimiento y Monitoreo Regular del Cableado

a) Se establecerá un programa de mantenimiento y monitoreo regular del cableado para detectar y abordar problemas potenciales a tiempo.

b) Se llevarán registros detallados de todas las actividades de mantenimiento realizadas, incluyendo inspecciones, reparaciones y mejoras.

11.4 Protección contra Riesgos Ambientales y Desastres Naturales

a) Se implementarán medidas de protección para salvaguardar el cableado contra riesgos ambientales, como incendios, inundaciones y terremotos.

b) Se desarrollará un plan de contingencia específico para el cableado, incluyendo medidas de respuesta en caso de desastres naturales u otros eventos imprevistos.

11.5 Capacitación y Concientización del Personal en Seguridad del Cableado

a) Se proporcionará capacitación regular a los empleados sobre prácticas seguras relacionadas con el manejo y cuidado del cableado.

b) Se promoverá la conciencia sobre la importancia de reportar cualquier anomalía o daño en el cableado de manera oportuna.

12. Mantenimiento de Equipos

Objetivo

Evitar la pérdida, daño, robo o compromiso de la información y otros activos asociados y la interrupción de las operaciones de la organización causada por la falta de mantenimiento.

12.1 Implementación de Programa de Mantenimiento Preventivo

a) Se establecerá y promoverá un programa de mantenimiento preventivo para garantizar el funcionamiento óptimo y continuo de los equipos.

b) Se identificarán los intervalos de mantenimiento recomendados y se llevará un registro detallado de las actividades realizadas.

12.2 Mantenimiento Correctivo Oportuno

a) Se implementará un proceso eficiente para el manejo de solicitudes y realización de mantenimiento correctivo en caso de fallas.

b) El personal encargado de mantenimiento estará disponible y capacitado para abordar problemas de manera oportuna y efectiva.

12.3 Seguridad de Datos Durante el Mantenimiento

a) Se establecerán procedimientos para garantizar la seguridad de los datos y la confidencialidad durante las actividades de mantenimiento.

b) Se brindará capacitación al personal de mantenimiento sobre la importancia de proteger la información mientras se trabaja en los equipos.

12.4 Registro y Documentación de Actividades de Mantenimiento

a) Se llevarán registros detallados de todas las actividades de mantenimiento realizadas, incluyendo fechas, descripciones y resultados.

b) Los informes de mantenimiento serán archivados de manera organizada y estarán disponibles para consulta y auditorías internas.

12.5 Planificación de Mantenimiento en Caso de Interrupciones

a) Se desarrollará un plan de contingencia que contemple el mantenimiento necesario en momentos de menor actividad para minimizar interrupciones.

b) Se coordinará con los departamentos pertinentes para planificar el mantenimiento de manera que afecte lo menos posible las operaciones críticas.

12.6 Capacitación y Concientización del Personal en Mantenimiento de Equipos

a) Se brindará capacitación regular a los empleados sobre la importancia del mantenimiento adecuado de los equipos y su impacto en la operación.

b) Se fomentará la conciencia sobre la responsabilidad de reportar problemas o necesidades de mantenimiento de manera proactiva.

13. Eliminación Segura o Reutilización de Equipos

Objetivo

Evitar la fuga de información de los equipos que se desecharán o reutilizarán.

13.1 Establecimiento de Procedimientos para la Eliminación Segura o Reutilización de Equipos

a) Se establecerán procedimientos detallados para asegurar la eliminación segura o la reutilización adecuada de equipos obsoletos o no necesarios.

b) Se definirán responsabilidades claras para supervisar y aprobar la eliminación o reutilización de equipos, garantizando la integridad de los datos.

13.2 Proceso de Eliminación Segura de Equipos

a) Se implementará un proceso de eliminación seguro que incluya la eliminación física y la destrucción de datos almacenados en los equipos.

b) Se utilizarán métodos certificados de borrado o destrucción, como el formateo seguro o la trituración, para garantizar la eliminación completa de la información.

13.3 Reutilización Responsable de Equipos

a) Se establecerán criterios claros para la reutilización de equipos, asegurando que se elimine adecuadamente la información previa antes de su reasignación.

b) Se llevarán registros detallados de los equipos reutilizados, incluyendo las acciones tomadas para eliminar o transferir la información.

13.4 Protección de Datos Durante el Proceso de Eliminación o Reutilización

a) Se implementarán medidas de seguridad para proteger la información durante el proceso de eliminación o reutilización de equipos.

b) Se brindará capacitación al personal involucrado en el manejo de equipos obsoletos, destacando la importancia de la protección de datos.

13.5 Auditorías y Seguimiento del Proceso de Eliminación o Reutilización

a) Se realizarán auditorías periódicas para verificar el cumplimiento de los procedimientos de eliminación segura y reutilización responsable.

b) Los informes de auditoría se presentarán a la alta dirección para garantizar la transparencia y la toma de decisiones informadas.

13.6 Capacitación y Concientización del Personal en Eliminación Segura o Reutilización de Equipos

a) Se proporcionará capacitación regular a los empleados sobre los procedimientos adecuados para la eliminación o reutilización de equipos.

b) Se promoverá la conciencia sobre la importancia de prevenir la fuga de información y garantizar la protección de datos durante estos procesos.

Referencias

ISO/IEC. (2022). ISO/IEC 27002:2022 Tecnología de la información — Técnicas de seguridad — Código de práctica para los controles de seguridad de la información.

Control de cambios

Control de cambios y versiones				
Versión	Fecha de versión	Motivo de la actualización	Nombre del encargado(s)	Firma
01	12-03-2023	Creación de las políticas	William García Molina	

		de seguridad físicas.	Michelle Rodríguez Hernández	

Anexo 8: Políticas de seguridad tecnológicas Distribuidora COARSA

POLÍTICAS DE SEGURIDAD TECNOLÓGICA

NORMA ISO 27002:2022

DPTO. INFORMÁTICA

Código: 07.3-MP-01

Versión 1.0

San Ramón, Costa Rica

Mayo, 2023

CONTENIDO

SIGLAS, ABREVIATURAS Y CONCEPTOS

WETRANSFER: aplicación basada en la transferencia de archivos especialmente pesados, por medio de la nube.

DROPBOX: Herramienta que permite sincronizar archivos a través de un directorio virtual o disco duro virtual de la red.

GOOGLE DRIVE: Servicio de alojamiento de archivos.

FTP: (File Transfer Protocol) es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red.

RESUMEN

El propósito de este documento es proporcionar a la organización una guía detallada basada en una serie de controles de seguridad centrados en dispositivos de punto final. Estos controles se han desarrollado con el objetivo de proteger la información contra los riesgos asociados con el uso de estos dispositivos por parte de los usuarios.

En colaboración con los responsables de Tecnologías de la Información de la organización, se ha seleccionado cuidadosamente una serie de controles tecnológicos basados en la Norma ISO 27002:2022 que se consideran fundamentales para mitigar los riesgos y fortalecer la ciberseguridad de la empresa. Estos controles abordan aspectos clave como los derechos de acceso privilegiado, la restricción de acceso a la información, la autenticación segura y la protección contra software malicioso, entre otros.

La implementación de estos controles permitirá a la organización garantizar que solo los usuarios autorizados tengan derechos de acceso privilegiado, prevenir el acceso no autorizado a la información, evitar la introducción de funciones no autorizadas y mantener la confidencialidad de la propiedad intelectual valiosa.

Además, estos controles contribuirán a detectar y prevenir la divulgación no autorizada de información, permitir la recuperación de la pérdida de datos o sistemas a través de copias de seguridad y asegurar el funcionamiento continuo de las instalaciones de procesamiento de información.

Al seguir estas políticas de seguridad basadas en los controles de dispositivos de punto final, la organización podrá fortalecer su postura de seguridad, proteger sus activos de información y salvaguardar la confidencialidad, integridad y disponibilidad de los datos críticos. Asimismo, se fomentará una cultura de seguridad en toda la empresa, involucrando a todos los empleados en la protección activa de la información y en la prevención de posibles brechas de seguridad.

INTRODUCCIÓN

La ciberseguridad se ha convertido en la era digital actual en una preocupación crítica para las empresas en todo el mundo. Los ataques cibernéticos están en constante aumento y representan una amenaza significativa para los activos de información de las organizaciones. Este documento proporciona una guía detallada basada en el capítulo 8 de la Norma ISO 27002:2022, reconocida internacionalmente como una referencia en materia de seguridad de la información. La Norma establece una serie de controles y buenas prácticas que las organizaciones pueden implementar para fortalecer su postura en seguridad cibernética.

La guía presentada en este documento abarca una amplia gama de aspectos relacionados con la ciberseguridad, desde la protección de dispositivos de punto final hasta la gestión de cambios y la seguridad de redes. Cada control y política propuestos han sido cuidadosamente seleccionados para adaptarse a las

necesidades específicas de la organización y cumplir con los estándares establecidos por la Norma ISO 27002:2022.

Al seguir esta guía y aplicar los controles recomendados, las organizaciones podrán fortalecer su capacidad para prevenir, detectar y responder a los ataques cibernéticos. Además, se fomentará una cultura de seguridad en toda la empresa, involucrando a todos los empleados en la protección activa de los activos de información y en la prevención de posibles brechas de seguridad.

OBJETIVO

El objetivo principal de esta guía es proporcionar a la organización una orientación detallada basada en la Norma ISO 27002:2022, con el fin de fortalecer su postura de ciberseguridad y proteger sus activos de información contra las amenazas y riesgos cibernéticos en constante evolución. La guía tiene como propósito ayudar a la empresa a implementar controles y prácticas recomendadas para garantizar la integridad, confidencialidad y disponibilidad de su información, así como prevenir posibles incidentes de seguridad y minimizar su impacto en el negocio.

ALCANCE

El alcance de este documento abarca la definición y descripción de un conjunto de controles tecnológicos, compuestos por un total de 21 medidas cuidadosamente seleccionadas por los creadores de esta guía, en colaboración con los responsables de Tecnologías de la Información de la Organización. Estos controles tecnológicos cubren una amplia gama de aspectos clave relacionados con la ciberseguridad y la protección de los activos de información de la organización.

MARCO DE REFERENCIA

El presente documento se enmarca en la Norma ISO 27002:2022, la cual establece los requisitos para el establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información. Los controles tecnológicos propuestos en este documento están alineados con los principios y las buenas prácticas establecidas en esta norma internacional. Su objetivo es garantizar que la organización cumpla con los estándares internacionales y las mejores prácticas en materia de seguridad de la información.

Esta política toma en consideración las necesidades y características específicas de la Organización, adaptándose a su entorno particular. Los controles tecnológicos descritos en este documento han sido cuidadosamente seleccionados para abordar los desafíos actuales en ciberseguridad y proteger los activos de información de la Organización.

Al seguir las políticas y controles tecnológicos aquí descritos, la Organización fortalecerá su postura de seguridad cibernética, reduciendo la probabilidad de sufrir incidentes relacionados con la seguridad de la información. Además, se fomentará una cultura de seguridad en toda la empresa, involucrando a todos los empleados en la protección activa de los activos de información y en la prevención de posibles brechas de seguridad.

Este marco de referencia se basa en la Norma ISO 27002:2022 y se adapta a las necesidades específicas de la Organización, proporcionando una guía

detallada para la implementación de controles tecnológicos eficaces y alineados con las mejores prácticas internacionales.

Políticas de seguridad de la información: controles tecnológicos

1. Dispositivos de punto final

Objetivo

Proteger la información contra los riesgos introducidos por el uso de dispositivos de punto final de usuario.

1.1 Uso de Dispositivos Aprobados

a. Se permite el uso de dispositivos de punto final aprobados por la organización, que cumplen con los estándares de seguridad establecidos.

b. Los dispositivos no aprobados no deben utilizarse para acceder a la red de la organización o para procesar información sensible.

c. Se mantendrá una lista actualizada de los dispositivos de punto final aprobados, incluyendo sus especificaciones técnicas y configuraciones permitidas.

1.2 Política de Autorización de Acceso

a. Solo se permitirá el acceso a la red y a los recursos de la organización a través de dispositivos de punto final autorizados y registrados.

b. Los usuarios deben obtener la autorización previa para acceder a la red mediante sus dispositivos de punto final y se llevará un registro de dichas autorizaciones.

c. El acceso a la red se revocará inmediatamente cuando se detecte un dispositivo de punto final no autorizado o comprometido.

1.3 Actualización de Software y Parches

a. Todos los dispositivos de punto final deben tener instaladas las últimas actualizaciones de software y parches de seguridad para mitigar las vulnerabilidades conocidas.

b. Se implementará un proceso regular de actualización y parcheo de software en los dispositivos de punto final para mantenerlos protegidos y asegurar su compatibilidad con las políticas de seguridad.

1.4 Protección contra Malware

a. Se utilizará un software antivirus y antimalware actualizado en todos los dispositivos de punto final y se realizarán análisis periódicos para detectar y eliminar cualquier amenaza.

b. Los usuarios deben estar capacitados para reconocer y evitar el acceso a sitios web o descargas potencialmente maliciosas que puedan comprometer la seguridad de los dispositivos de punto final.

1.5 Política de Contraseñas

a. Se establecerá una política sólida de contraseñas para los dispositivos de punto final, incluyendo la longitud mínima, la complejidad de caracteres y la frecuencia de cambio de contraseñas.

b. Se recomendará el uso de contraseñas únicas y el empleo de autenticación de dos factores para reforzar la seguridad de los dispositivos de punto final.

1.6 Cifrado de Datos

a. Se requerirá el cifrado de datos confidenciales almacenados en los dispositivos de punto final, especialmente en aquellos utilizados fuera de las instalaciones de la organización.

b. Se utilizarán algoritmos robustos de cifrado y se implementarán medidas adicionales de seguridad, como la autenticación de dos factores, cuando sea necesario, para asegurar la confidencialidad de la información almacenada en los dispositivos.

1.7 Política de Uso Aceptable

a. Se establecerá una política de uso aceptable que defina claramente las actividades permitidas y restringidas en los dispositivos de punto final.

b. Los usuarios deben ser conscientes de sus responsabilidades y cumplir con las políticas establecidas para el uso adecuado de los dispositivos de punto final, evitando el acceso a contenido no autorizado o peligroso.

1.8 Capacitación y Concientización

a. Se proporcionará capacitación y concientización periódica a los usuarios sobre las mejores prácticas de seguridad relacionadas con el uso de dispositivos de punto final.

b. Los usuarios deben ser conscientes de los riesgos asociados con el uso inadecuado de los dispositivos de punto final y estar preparados para actuar de manera segura.

c. Se promoverá la educación sobre la identificación de amenazas comunes, el uso seguro de contraseñas, la detección de *phishing* y la protección de la información confidencial almacenada en los dispositivos de punto final.

1.9 Política de Copias de Seguridad

a. Se establecerá una política de copias de seguridad regular de los datos almacenados en los dispositivos de punto final.

b. Se determinarán los intervalos de tiempo y la ubicación adecuada para realizar las copias de seguridad, asegurando que los datos estén protegidos y sean recuperables en caso de pérdida o daño del dispositivo.

1.10 Monitoreo y Detección de Actividades Anómalas

a. Se implementarán herramientas de monitoreo y detección de actividad anómala en los dispositivos de punto final.

b. Se realizará un seguimiento constante de los registros de actividad y se investigarán cualquier anomalía o comportamiento sospechoso.

c. Se establecerán mecanismos de alerta temprana para responder rápidamente a posibles amenazas o incidentes de seguridad.

1.11 Responsabilidad y Notificación de Incidentes

a. Se establecerá un proceso claro y definido para la notificación de incidentes de seguridad relacionados con los dispositivos de punto final.

b. Los usuarios deberán informar de inmediato cualquier incidente o brecha de seguridad a los responsables designados dentro de la organización.

c. Se llevará a cabo una investigación exhaustiva de los incidentes reportados y se implementarán medidas correctivas y preventivas apropiadas.

1.12 Evaluación y Auditoría

a. Se realizarán evaluaciones regulares de la seguridad de los dispositivos de punto final para identificar posibles vulnerabilidades y deficiencias.

b. Se llevarán a cabo auditorías internas o externas para verificar el cumplimiento de las políticas de seguridad y evaluar la eficacia de los controles implementados.

2. Derechos de acceso privilegiado

Objetivo: garantizar que solo los usuarios autorizados, los componentes y servicios de software reciban derechos de acceso privilegiado.

2.1 Identificación y Gestión de Usuarios Autorizados

a. Se establecerá un proceso riguroso de identificación y autenticación de usuarios autorizados que requieran derechos de acceso privilegiado. Esto incluirá la verificación de la identidad, la validación de los privilegios necesarios y la aprobación por parte de los responsables correspondientes.

b. Se llevará a cabo una revisión periódica de los usuarios con derechos de acceso privilegiado para asegurarse de que sigan siendo autorizados y necesarios para sus funciones. Además, se implementarán controles de separación de funciones para evitar la acumulación excesiva de privilegios.

2.2 Política de Mínimos Privilegios

a. Se establecerá un procedimiento estricto de mínimos privilegios, con el cual, los usuarios solo recibirán los privilegios de acceso necesarios para llevar a cabo sus tareas y responsabilidades. Se evitará otorgar privilegios excesivos o innecesarios, lo que reducirá el riesgo de posibles abusos o mal uso de los derechos de acceso privilegiado.

b. Se requerirá una justificación y aprobación adecuada para solicitar nuevos derechos de acceso privilegiado. Estas solicitudes deberán ser evaluadas y

aprobadas por los responsables correspondientes, teniendo en cuenta los principios de necesidad y proporcionalidad.

2.3 Control y Monitoreo de Acceso Privilegiado

a. Se implementarán controles técnicos y procedimientos de monitoreo para registrar y auditar los accesos privilegiados. Esto permitirá detectar y rastrear actividades sospechosas o no autorizadas, así como realizar investigaciones posteriores en caso de incidentes.

b. Se llevará a cabo un monitoreo continuo de las actividades realizadas con derechos de acceso privilegiado para identificar posibles abusos, mal uso o comportamientos inusuales. Esto ayudará a garantizar que los usuarios estén utilizando sus privilegios de manera adecuada y acorde con sus responsabilidades asignadas.

2.4 Gestión de Contraseñas

a. Se establecerán procedimientos claros para la gestión segura de las contraseñas asociadas con los derechos de acceso privilegiado. Esto incluirá la exigencia de contraseñas robustas, la prohibición de compartir contraseñas y la implementación de medidas de protección, como el cifrado de contraseñas.

b. Se requerirá un cambio periódico de contraseñas y se implementarán mecanismos de verificación de fortaleza de contraseñas para garantizar su integridad y seguridad.

2.5 Separación de Funciones

a. Se promoverá una clara separación de funciones entre los usuarios con derechos de acceso privilegiado. Esto implicará asignar roles y responsabilidades específicos y limitar la acumulación excesiva de privilegios en un solo usuario. La separación de funciones reduce el riesgo de posibles conflictos de interés y minimiza la exposición a amenazas internas.

3.Restricción de acceso a la información

Objetivo: garantizar solo el acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados.

3.1 Acceso autorizado

a. Solo los usuarios autorizados tendrán acceso a la información y los activos asociados.

b. Se establecerán procedimientos para verificar y validar la identidad de los usuarios antes de otorgarles acceso.

3.2 Clasificación de información

a. Se clasificará la información en categorías según su nivel de sensibilidad y se establecerán controles de acceso adecuados basados en esta clasificación.

b. Se identificarán los roles y permisos necesarios para acceder a cada categoría de información.

3.3 Control de acceso

a. Se implementarán medidas técnicas y organizativas para controlar el acceso a la información, como autenticación, autorización y cifrado.

b. Se establecerán procedimientos para administrar los derechos de acceso y garantizar que se otorguen de acuerdo con las necesidades y responsabilidades de los usuarios.

3.4 Gestión de contraseñas

a. Se requerirá el uso de contraseñas seguras y se establecerán políticas para su creación, cambio regular y almacenamiento seguro.

b. Se fomentará la educación y concienciación sobre las mejores prácticas para el uso de contraseñas.

3.5 Control de acceso físico

a. Se establecerán medidas de seguridad física, como tarjetas de acceso, cerraduras y vigilancia, para restringir el acceso a las áreas donde se almacena la información sensible.

b. Se implementarán procedimientos para la gestión de visitantes y el control de acceso de proveedores externos.

3.6 Revisión y auditoría

a. Se realizarán revisiones periódicas de los derechos de acceso para garantizar que sigan siendo apropiados y necesarios.

b. Se llevarán a cabo auditorías de seguridad para evaluar la eficacia de los controles de acceso y detectar posibles deficiencias.

4. Acceso al código fuente

Objetivo: evitar la introducción de funciones no autorizadas, evitar cambios no intencionales o maliciosos y mantener la confidencialidad de la propiedad intelectual valiosa.

4.1 Control de acceso y autorización

a. Solo los usuarios autorizados tendrán acceso al código fuente de las bases de datos.

b. Se establecerán procedimientos para verificar y validar la identidad de los usuarios antes de otorgarles acceso al código fuente.

c. Se asignarán roles y permisos específicos para el acceso al código fuente, asegurándose de que solo los usuarios necesarios tengan privilegios para modificar o visualizar el código.

4.2 Segregación de funciones

a. Se implementarán medidas para garantizar la segregación de funciones, evitando que una sola persona tenga acceso y control total sobre el código fuente de las bases de datos.

b. Se definirán roles y responsabilidades claras para el manejo del código fuente, incluyendo la revisión y aprobación de los cambios realizados.

4.3 Control de versiones

a. Se utilizará un sistema de control de versiones para gestionar y rastrear los cambios realizados en el código fuente de las bases de datos.

b. Se registrarán los cambios realizados, incluyendo información sobre el autor, la fecha y la descripción de los cambios efectuados.

4.4 Proceso de revisión y aprobación

a. Se establecerá un proceso formal de revisión y aprobación para los cambios en el código fuente de las bases de datos.

b. Antes de implementar cualquier modificación, se requerirá una revisión exhaustiva por parte de un equipo designado, asegurando la integridad y la calidad del código.

4.5 Monitorización y detección de cambios no autorizados

a. Se implementarán sistemas y herramientas de monitorización para detectar cambios no autorizados o inesperados en el código fuente de las bases de datos.

b. Se establecerán alertas y registros de auditoría para identificar y responder rápidamente a cualquier actividad sospechosa o no autorizada.

4.6 Protección de la propiedad intelectual

a. Se tomarán medidas para proteger la confidencialidad y propiedad intelectual valiosa contenida en el código fuente de las bases de datos.

b. Se aplicarán técnicas de encriptación y control de acceso adicional para salvaguardar la información sensible y prevenir su divulgación no autorizada.

5. Autenticación segura

Objetivo: garantizar que un usuario o una entidad se autentica de forma segura cuando se otorga acceso a sistemas, aplicaciones y servicios.

5.1 Contraseñas Seguras

a. Se requerirá el uso de contraseñas fuertes para todos los usuarios, con una combinación de letras mayúsculas y minúsculas, números y caracteres especiales.

b. Se establecerá una política de cambio regular de contraseñas, con una frecuencia determinada y comunicada a todos los usuarios.

c. Se desaconsejará el uso de contraseñas obvias o fáciles de adivinar, como fechas de nacimiento, nombres de familiares o palabras comunes.

5.2 Autenticación Multifactor

a. Se implementará la autenticación multifactor (MFA) en todos los sistemas y aplicaciones que contengan información sensible o crítica.

b. Se requerirá que los usuarios proporcionen al menos dos factores de autenticación, como una contraseña y un código generado por una aplicación de autenticación móvil.

c. Se promoverá el uso de tecnologías biométricas, como huellas dactilares o reconocimiento facial, como un factor adicional de autenticación cuando sea posible.

5.3 Gestión de Credenciales

a. Se establecerá un proceso seguro y controlado para la creación, distribución y gestión de credenciales de acceso, como nombres de usuario y contraseñas.

b. Se utilizarán mecanismos seguros para almacenar y transmitir las credenciales de forma cifrada, evitando la exposición no autorizada de información de autenticación.

c. Se implementarán políticas de revocación y eliminación de credenciales para usuarios que dejen de tener acceso autorizado.

5.4 Control de Acceso Basado en Roles

a. Se implementará un sistema de control de acceso basado en roles, en el cual se asignen permisos y privilegios de acuerdo con las responsabilidades y necesidades de cada usuario.

b. Se revisarán y actualizarán regularmente los roles y permisos asignados, asegurándose de que los usuarios solo tengan acceso a los recursos necesarios para realizar sus funciones.

c. Se realizarán auditorías periódicas para verificar el cumplimiento de las políticas de control de acceso y para detectar y corregir cualquier desviación o abuso de privilegios.

6. Protección contra software malicioso

Objetivo: garantizar que la información y otros activos asociados estén protegidos contra *malware.*

6.1 Prevención de Infecciones de *Malware*

a. Se implementarán soluciones de seguridad, como software antivirus y *antimalware*, en todos los sistemas y dispositivos utilizados dentro de la organización.

b. Se realizarán actualizaciones periódicas de las bases de datos de firmas y definiciones de *malware* para garantizar una protección efectiva contra las amenazas más recientes.

c. Se establecerá una política de escaneo regular de archivos y dispositivos para detectar y eliminar cualquier software malicioso presente.

6.2 Restricción de Descargas y Ejecución de Software

a. Se establecerán políticas y mecanismos para restringir la descarga y ejecución de software no autorizado o de fuentes desconocidas en los sistemas de la organización.

b. Se promoverá el uso de fuentes confiables y verificadas para la descarga de software, como tiendas oficiales y proveedores reconocidos.

c. Se educará a los usuarios sobre los riesgos asociados con la descarga y ejecución de software no autorizado o de dudosa procedencia.

6.3 Actualización y Parcheo de Software

a. Se establecerá un proceso de actualización y parcheo regular de todos los sistemas y aplicaciones utilizados en la organización.

b. Se priorizarán las actualizaciones de seguridad que aborden vulnerabilidades conocidas y que puedan ser explotadas por *malware*.

c. Se realizarán pruebas y evaluaciones de compatibilidad antes de implementar cualquier actualización o parche, para minimizar el impacto en la operatividad de los sistemas.

6.4 Concientización y Entrenamiento de Usuarios

a. Se llevarán a cabo programas de concientización y capacitación regular para educar a los usuarios sobre las mejores prácticas de seguridad, incluyendo la identificación y prevención de *malware*.

b. Se proporcionarán directrices claras sobre cómo reconocer correos electrónicos o enlaces sospechosos, así como el manejo adecuado de archivos adjuntos y dispositivos externos.

c. Se fomentará una cultura de seguridad cibernética entre los usuarios, promoviendo la responsabilidad individual en la protección contra el *malware*.

7. Gestión de vulnerabilidades técnicas

Objetivo: prevenir la explotación de vulnerabilidades técnicas.

7.1 Identificación de Vulnerabilidades

a. Se realizarán evaluaciones regulares de vulnerabilidades en los sistemas y aplicaciones utilizados en la organización, utilizando herramientas de escaneo y pruebas de seguridad.

b. Se establecerá un proceso para identificar y documentar las vulnerabilidades identificadas, asignándoles una prioridad en función de su gravedad y potencial impacto.

7.2 Parcheo y Actualización de Software

a. Se establecerá un programa de parcheo regular y actualización de software, que incluya tanto los sistemas operativos como las aplicaciones utilizadas en la organización.

b. Se dará prioridad a la aplicación de parches de seguridad que aborden vulnerabilidades conocidas y que puedan ser explotadas por actores malintencionados.

c. Se realizarán pruebas y evaluaciones de compatibilidad antes de implementar cualquier actualización o parche, para minimizar el impacto en la operatividad de los sistemas.

7.3 Gestión de Versiones y Configuraciones

a. Se establecerá un proceso de gestión de versiones y configuraciones para garantizar que los sistemas y aplicaciones se mantengan actualizados y configurados de manera segura.

b. Se controlará y registrará cualquier cambio realizado en la configuración de los sistemas y aplicaciones, asegurándose de que se realicen de acuerdo con las mejores prácticas de seguridad.

7.4 Mitigación de Vulnerabilidades

a. Se implementarán medidas de mitigación para abordar las vulnerabilidades identificadas, como la aplicación de controles adicionales, la restricción de accesos o la segmentación de redes.

b. Se establecerá un proceso para monitorear y evaluar regularmente la efectividad de las medidas de mitigación implementadas, realizando ajustes según sea necesario.

7.5 Concientización y Capacitación

a. Se llevarán a cabo programas de concientización y capacitación para educar a los usuarios sobre la importancia de la gestión de vulnerabilidades y las mejores prácticas para prevenir su explotación.

b. Se proporcionará información y recursos para que los usuarios reporten rápidamente cualquier vulnerabilidad o incidente de seguridad detectado.

8. Gestión de la configuración

Objetivo: garantizar que el hardware, el software, los servicios y las redes funcionen correctamente con la configuración de seguridad requerida y que la configuración no se altere por cambios no autorizados o incorrectos.

8.1 Identificación y Documentación de Configuraciones

a. Se realizará un inventario de todos los activos de hardware, software, servicios y redes utilizados en la organización, documentando su configuración de seguridad requerida.

b. Se mantendrá un registro actualizado de las configuraciones establecidas, incluyendo información relevante como versiones de software, configuraciones de red y parámetros de seguridad.

8.2 Establecimiento de Configuraciones Seguras

a. Se definirán estándares y directrices claras para la configuración segura de hardware, software, servicios y redes, basadas en mejores prácticas y requisitos de seguridad.

b. Se implementarán controles y medidas de seguridad adecuadas para garantizar que los activos se configuren de acuerdo con los estándares establecidos.

c. Se realizarán revisiones periódicas para verificar y asegurar que los activos se mantengan correctamente configurados y alineados con las políticas de seguridad.

8.3 Control de Cambios de Configuración

a. Se establecerá un proceso formal de control de cambios para gestionar cualquier modificación en la configuración de los activos.

b. Se requerirá una revisión y aprobación previa antes de implementar cualquier cambio de configuración, asegurando que se realicen de manera autorizada y correcta.

c. Se registrarán todos los cambios de configuración realizados, incluyendo detalles como la fecha, el responsable y la justificación del cambio.

8.4 Monitorización y Auditoría de Configuraciones

a. Se implementarán herramientas y sistemas de monitorización para detectar cambios no autorizados o inesperados en las configuraciones de los activos.

b. Se establecerán registros de auditoría para registrar y revisar las modificaciones de configuración, facilitando la identificación de cambios no autorizados o incorrectos.

c. Se realizarán auditorías periódicas de configuración para evaluar el cumplimiento de los estándares y directrices establecidos.

8.5 Gestión de Versiones de Configuración:

a. Se utilizará un sistema de gestión de versiones para controlar y rastrear los cambios realizados en la configuración de los activos.

b. Se mantendrán copias de seguridad y puntos de restauración de las configuraciones establecidas, permitiendo la recuperación en caso de cambios no deseados o incidentes.

9. Eliminación de información

Objetivo: evitar la exposición innecesaria de información confidencial y cumplir con los requisitos legales, estatuarios y reglamentarios y contractuales para la eliminación de información.

9.1 Gestión de Ciclo de Vida de la Información

a. Se establecerán procedimientos y directrices para la gestión adecuada del ciclo de vida de la información, desde su creación hasta su eliminación.

b. Se categorizará la información según su nivel de confidencialidad y se aplicarán políticas de retención de acuerdo con los requisitos legales, estatutarios, reglamentarios y contractuales.

9.2 Identificación y Clasificación de Información a Eliminar

a. Se realizará un inventario de la información almacenada en los sistemas y dispositivos de la organización, identificando los datos que deben eliminarse de manera segura.

b. Se establecerá un proceso de clasificación de la información, determinando qué datos son confidenciales y deben protegerse de forma especial durante la eliminación.

9.3 Procedimientos de Eliminación Segura

a. Se implementarán métodos y herramientas para la eliminación segura de la información, incluyendo técnicas de borrado seguro, destrucción física o criptografía según corresponda.

b. Se establecerán controles y medidas para garantizar que la información eliminada no pueda recuperarse de forma indebida.

9.4 Gestión de Dispositivos y Medios de Almacenamiento

a. Se implementarán políticas y procedimientos para la gestión adecuada de dispositivos y medios de almacenamiento que contengan información sensible.

b. Se establecerán reglas claras sobre el uso, la protección y la eliminación de dispositivos y medios de almacenamiento, asegurando que se sigan prácticas seguras en todo momento.

9.5 Formación y Concienciación del Personal

a. Se proporcionará formación y concienciación regular al personal sobre la importancia de la eliminación segura de información confidencial.

b. Se promoverá una cultura de seguridad que fomente la responsabilidad individual en la eliminación adecuada de la información.

9.6 Registro y Auditoría de Eliminación

a. Se llevará un registro de todas las actividades de eliminación de información, incluyendo detalles como la fecha, el tipo de información y la persona responsable.

b. Se realizarán auditorías periódicas para verificar el cumplimiento de las políticas de eliminación de información y garantizar su efectividad.

10. Prevención de fuga de datos

Objetivo: detectar y prevenir la divulgación y extracción no autorizada de información por parte de individuos o sistemas.

10.1 Gestión de Políticas de Seguridad de la Información

a. Se establecerán políticas claras y documentadas para la prevención de fuga de datos que incluyan la protección de información confidencial y la prohibición de su divulgación no autorizada.

b. Las políticas de seguridad de la información serán comunicadas y entrenadas a todos los empleados, para asegurar su comprensión y cumplimiento.

10.2 Implementación de Medidas de Protección

a. Se utilizarán tecnologías y herramientas de seguridad de la información, como *firewalls*, sistemas de prevención de pérdida de datos (DLP), cifrado y monitoreo de actividad, para detectar y prevenir la fuga de datos.

b. Se establecerán mecanismos de control para monitorear y registrar el acceso a información sensible, identificar actividades sospechosas y responder de manera adecuada a incidentes de fuga de datos.

10.3 Gestión de Identificación y Acceso

a. Se implementarán medidas de autenticación y control de acceso para garantizar que solo los usuarios autorizados tengan acceso a la información confidencial.

b. Se establecerán políticas de gestión de contraseñas, como la utilización de contraseñas fuertes, el cambio periódico de contraseñas y la restricción de acceso a cuentas privilegiadas.

10.4 Educación y Concientización del Personal

a. Se proporcionará capacitación periódica a los empleados sobre las mejores prácticas de seguridad de la información y la importancia de prevenir la fuga de datos.

b. Se promoverá una cultura de seguridad en la organización, fomentando la responsabilidad individual y el compromiso con la protección de la información confidencial.

10.5 Monitoreo y Detección de Actividades Anómalas

a. Se implementarán soluciones de monitoreo y detección de anomalías para identificar patrones de comportamiento inusuales y actividades sospechosas que puedan indicar una posible fuga de datos.

b. Se establecerán alertas y procedimientos de respuesta ante posibles incidentes de fuga de datos, para minimizar el impacto y tomar acciones correctivas rápidamente.

10.6 Revisión y Actualización de Políticas

a. Se realizarán revisiones periódicas de las políticas de prevención de fuga de datos, con el fin de evaluar su efectividad y realizar mejoras o ajustes según sea necesario.

b. Se mantendrá actualizada la lista de información confidencial y se revisarán regularmente los permisos de acceso a dicha información, asegurando que solo las personas autorizadas tengan acceso.

11. Copias de seguridad de la información

Objetivo: permitir la recuperación de la pérdida de datos o sistemas.

11.1 Planificación y Programación de Copias de Seguridad

a. Se establecerá un plan de copias de seguridad que incluya la programación regular y la realización de copias de seguridad de los datos y sistemas críticos.

b. Se identificarán los datos y sistemas prioritarios que requieren copias de seguridad y se establecerán los intervalos de tiempo adecuados para su respaldo.

c. Se definirán los procedimientos de retención de copias de seguridad, determinando el período de tiempo durante el cual las copias se mantendrán en almacenamiento.

11.2 Almacenamiento Seguro de las Copias de Seguridad

a. Las copias de seguridad se almacenarán en ubicaciones físicas o en servicios seguros de almacenamiento en la nube, protegidos contra accesos no autorizados, daños físicos o desastres naturales.

b. Se establecerán medidas de seguridad adicionales, como el cifrado de las copias de seguridad, para garantizar la confidencialidad e integridad de los datos almacenados.

c. Se realizarán copias de seguridad en diferentes ubicaciones geográficas para evitar la pérdida de datos, debido a un solo punto de falla.

11.3 Pruebas de Restauración

a. Se realizarán pruebas periódicas de restauración para verificar la eficacia y la integridad de las copias de seguridad, asegurando que los datos puedan recuperarse correctamente en caso de pérdida o fallos del sistema.

b. Se documentarán y se mantendrán registros de las pruebas de restauración realizadas, incluyendo los resultados y las acciones correctivas tomadas en caso de fallos.

c. Se establecerán procedimientos para la validación y verificación de la integridad de las copias de seguridad antes de su implementación en entornos de producción.

11.4 Control de Acceso a las Copias de Seguridad

a. El acceso a las copias de seguridad estará restringido únicamente a personal al autorizado, utilizando mecanismos de autenticación y control de acceso adecuados.

b. Se establecerán procedimientos de autorización y documentación para garantizar que solo las personas autorizadas tengan acceso y realicen cambios en las copias de seguridad.

c. Se implementarán registros de auditoría para monitorear y rastrear el acceso y las actividades relacionadas con las copias de seguridad.

11.5 Respaldo de Configuraciones y Ajustes del Sistema

a. Además de los datos, se realizarán copias de seguridad de las configuraciones y ajustes críticos del sistema, para permitir una recuperación completa y rápida en caso de fallos o pérdidas.

b. Se mantendrá una documentación actualizada de las configuraciones y ajustes respaldados, asegurando que sean consistentes con las necesidades operativas y de seguridad de la organización.

c. Se realizarán pruebas de restauración de las configuraciones y ajustes respaldados para verificar su integridad y su capacidad para restaurar el sistema a un estado funcional.

11.6 Revisión y Mejora Continua

a. Se llevará a cabo una revisión regular del plan de copias de seguridad y se realizarán mejoras o ajustes según sea necesario, para asegurar su alineación con los cambios tecnológicos y los requisitos de la organización.

b. Se realizará un seguimiento de las métricas de rendimiento de las copias de seguridad, como el tiempo de recuperación y la integridad de los datos, y se implementarán medidas correctivas para abordar cualquier brecha o problema identificado.

c. Se fomentará la conciencia y la capacitación del personal sobre las políticas y prácticas de copias de seguridad de la información, promoviendo una cultura de responsabilidad y cumplimiento.

11.7 Respaldo de Documentación y Procedimientos

a. Además de los datos y sistemas, se realizarán copias de seguridad de la documentación y los procedimientos críticos de la organización, asegurando la disponibilidad y la recuperación de la información necesaria para mantener la continuidad del negocio.

b. Se establecerá un proceso de gestión de versiones para las documentaciones y procedimientos respaldados, garantizando la actualización y la coherencia con las prácticas operativas y de seguridad vigentes.

c. Se realizarán pruebas periódicas de recuperación de la documentación y los procedimientos respaldados para verificar su integridad y su capacidad para respaldar las operaciones en caso de necesidad.

11.8 Consideraciones de Almacenamiento a Largo Plazo

a. Se establecerán políticas y procedimientos para el almacenamiento a largo plazo de las copias de seguridad, garantizando la preservación de los datos y su recuperación en períodos extendidos.

b. Se utilizarán tecnologías y medios de almacenamiento adecuados para minimizar el deterioro o la pérdida de datos durante el almacenamiento a largo plazo.

c. Se realizarán pruebas y verificaciones periódicas de las copias de seguridad almacenadas a largo plazo, para garantizar su integridad y su capacidad de recuperación en caso de necesidad.

12. Redundancia de las instalaciones de procesamiento de información

Objetivo: asegurar el funcionamiento continuo de las instalaciones de procesamiento de información.

12.1 Evaluación de la Infraestructura

a. Se realizará una evaluación exhaustiva de las instalaciones de procesamiento de información para identificar puntos únicos de falla y áreas de mejora en términos de redundancia.

b. Se considerarán elementos críticos como la alimentación eléctrica, la conectividad de red, el enfriamiento y la seguridad física en la planificación de la redundancia.

12.2 Implementación de Fuentes de Energía Redundantes

a. Se establecerá una configuración de fuentes de energía redundantes, como sistemas de alimentación ininterrumpida (UPS) y generadores de respaldo, para garantizar un suministro de energía continuo y confiable.

b. Se llevarán a cabo pruebas regulares de los sistemas de energía redundantes para verificar su funcionalidad y capacidad de conmutación sin interrupciones.

12.3 Redundancia de la Conectividad de Red

a. Se implementarán conexiones redundantes de red, como enlaces múltiples de Internet y rutas alternativas, para asegurar la disponibilidad y la continuidad del acceso a los servicios y sistemas de información.

b. Se realizarán pruebas periódicas de conmutación y conmutación automática para garantizar la capacidad de conmutación sin problemas entre las conexiones redundantes de red.

12.4 Redundancia del Enfriamiento

a. Se implementarán sistemas redundantes de enfriamiento, como unidades de aire acondicionado y sistemas de refrigeración, para mantener las temperaturas adecuadas en las instalaciones de procesamiento de información.

b. Se llevarán a cabo pruebas regulares de los sistemas redundantes de enfriamiento para garantizar su funcionamiento óptimo y su capacidad de mantener las condiciones ambientales adecuadas.

12.5 Seguridad Física Redundante

a. Se establecerán medidas redundantes de seguridad física, como sistemas de acceso y control de ingreso, cámaras de vigilancia y alarmas, para proteger las instalaciones de procesamiento de información contra amenazas externas.

b. Se realizarán pruebas periódicas de los sistemas redundantes de seguridad física para garantizar su funcionamiento efectivo y su capacidad de detectar y responder a situaciones de riesgo.

12.6 Evaluación y Selección de UPS del Centro de Datos

a. Se realizará una evaluación exhaustiva de las necesidades de energía del centro de datos y se seleccionará un sistema de alimentación ininterrumpida (UPS) adecuado.

b. Se considerarán factores como la capacidad de carga, la eficiencia energética, la escalabilidad y la capacidad de autonomía en caso de cortes de energía prolongados.

12.7 Implementación de UPS Redundantes

a. Se instalarán múltiples UPS en el centro de datos para proporcionar una fuente de energía de respaldo confiable en caso de interrupciones en el suministro eléctrico principal.

b. Se configurará un sistema de conmutación automática para garantizar una transición fluida y sin interrupciones entre el suministro eléctrico principal y el suministro de respaldo del UPS.

13. Registro

Objetivo: registrar eventos, generar evidencia, garantizar la integridad de la información de registro, prevenir el acceso no autorizado, identificar eventos de seguridad de la información que puedan conducir a un incidente de seguridad de la información y respaldar investigaciones.

13.1 Definición de Eventos a Registrar

a. Se establecerá una lista de eventos y actividades que deben registrarse, considerando los requisitos legales, reglamentarios y de cumplimiento aplicables.

b. Se incluirán eventos como inicio y cierre de sesión de usuarios, cambios en la configuración, acceso a recursos críticos, intentos de acceso no autorizado y errores del sistema, entre otros.

13.2 Implementación de Herramientas de Registro

a. Se utilizarán adecuados sistemas y herramientas de registro, como registros de eventos y sistemas de gestión de registros, para capturar y almacenar de manera segura la información relevante.

b. Se configurarán los parámetros adecuados de registro para capturar la información necesaria para el análisis y la investigación de eventos.

13.3 Seguridad y Protección de los Registros

a. Se establecerán medidas de seguridad para proteger los registros de eventos, incluyendo el acceso restringido a los archivos de registro y la encriptación de los datos almacenados.

b. Se implementarán copias de seguridad periódicas de los registros y se almacenarán en un lugar seguro, garantizando su disponibilidad y resiliencia ante posibles pérdidas o daños.

13.4 Análisis y Monitoreo de los Registros

a. Se realizará un análisis regular de los registros de eventos para detectar patrones o actividades inusuales que puedan indicar posibles incidentes de seguridad.

b. Se configurarán alertas y notificaciones para informar al personal de seguridad sobre eventos críticos o sospechosos que requieran una acción inmediata.

13.5 Retención y Eliminación de los Registros

a. Se establecerán políticas de retención de registros, basadas en los requisitos legales y regulatorios, para determinar el tiempo durante el cual los registros deban mantenerse almacenados.

b. Se establecerán procedimientos adecuados para la eliminación segura y definitiva de los registros, garantizando que no puedan recuperarse o utilizarse indebidamente una vez que hayan alcanzado su período de retención.

14. Actividades de seguimiento

Objetivo: detectar comportamientos anómalos y posibles incidentes de seguridad de la información.

14.1 Monitoreo de Actividades del Sistema

a. Se implementará un sistema de monitoreo continuo de las actividades del sistema, que registre y analice los eventos y comportamientos de los usuarios y los sistemas.

b. Se configurarán alertas y notificaciones para detectar actividades inusuales, como intentos de acceso no autorizado, modificaciones no

autorizadas de archivos o configuraciones y transferencias de datos sospechosas.

14.2 Análisis de Registros de Eventos

a. Se realizará un análisis regular de los registros de eventos generados por los sistemas y aplicaciones, con el fin de identificar posibles patrones o anomalías que indiquen actividades maliciosas.

b. Se utilizarán herramientas y técnicas de análisis de registros para extraer información relevante y detectar comportamientos anómalos.

14.3 Monitoreo de Tráfico de Red

a. Se implementarán soluciones de monitoreo de tráfico de red para analizar los flujos de datos y detectar actividades sospechosas, como intentos de intrusión, comunicaciones no autorizadas o transferencias de datos sensibles.

b. Se configurarán alertas y notificaciones para informar sobre patrones de tráfico inusuales o actividades anómalas en la red.

14.4 Supervisión de Accesos y Privilegios

a. Se realizará un seguimiento y monitoreo regular de los accesos y privilegios de los usuarios, asegurándose de que solo tengan acceso a los recursos y datos necesarios para realizar sus funciones.

b. Se registrarán y analizarán los cambios en los permisos y privilegios de los usuarios, con el fin de identificar modificaciones no autorizadas o abusos de privilegios.

14.5 Evaluación de Actividades de Usuarios

a. Se llevará a cabo una evaluación periódica de las actividades de los usuarios, revisando registros de inicio de sesión, patrones de uso de aplicaciones y recursos, y actividades realizadas en sistemas críticos.

b. Se buscarán comportamientos anómalos, como intentos repetidos de acceso no autorizado, acceso a recursos fuera de horarios establecidos o transferencias de datos inusuales.

15. Instalación de software en sistemas operativos

Objetivo: garantizar la integridad de los sistemas operativos y evitar la explotación de vulnerabilidades técnicas.

15.1 Autorización y Control de Software

a. Se establecerá un proceso de autorización formal para la instalación de software en los sistemas operativos, asegurándose de que solo se instalen aplicaciones aprobadas y confiables.

b. Se mantendrá un inventario actualizado de todo el software instalado en los sistemas operativos, incluyendo información relevante como la versión, el proveedor y los permisos asociados.

15.2 Verificación de Fuentes e Integridad del Software

a. Antes de instalar cualquier software en los sistemas operativos, se verificará la fuente y la autenticidad del software, evitando la instalación de aplicaciones provenientes de fuentes no confiables o potencialmente maliciosas.

b. Se comprobará la integridad del software mediante la comparación de las firmas digitales, los *hashes* o los controles de integridad establecidos por el proveedor del software.

15.3 Actualizaciones y Parches de Seguridad

a. Se establecerá un proceso regular de aplicación de actualizaciones y parches de seguridad en los sistemas operativos, con el fin de corregir vulnerabilidades conocidas y fortalecer la seguridad del sistema.

b. Se configurarán mecanismos automáticos de actualización o se asignarán responsabilidades claras para garantizar que las actualizaciones se implementen oportuna y efectivamente.

15.4 Evaluación de Riesgos y Pruebas de Compatibilidad

a. Antes de la instalación de cualquier software en los sistemas operativos, se realizarán evaluaciones de riesgos y pruebas de compatibilidad para identificar posibles conflictos, vulnerabilidades o impactos negativos en la estabilidad y seguridad del sistema.

b. Se documentarán los resultados de las evaluaciones y pruebas, y se tomarán las medidas correctivas apropiadas antes de proceder con la instalación.

15.5 Registro y Monitoreo de Actividades de Instalación

a. Se llevará un registro de todas las actividades de instalación de software en los sistemas operativos, incluyendo detalles como la fecha, el responsable y la descripción del software instalado.

b. Se implementará un monitoreo regular de las actividades de instalación, verificando que se cumplan los procedimientos establecidos y detectando posibles instalaciones no autorizadas o maliciosas.

16. Seguridad de redes

Objetivo: proteger la información en las redes y sus instalaciones de procesamiento de información de apoyo del compromiso a través de la red.

16.1 Segmentación de la Red

a. Se implementará una segmentación de red adecuada para separar los diferentes sistemas y recursos según su nivel de confidencialidad y criticidad.

b. Se establecerán *firewalls* y reglas de acceso para controlar el tráfico entre las diferentes segmentaciones de red y prevenir la propagación de ataques.

16.2 Control de Acceso a la Red

a. Se implementarán mecanismos de autenticación y autorización robustos para controlar el acceso a la red, asegurándose de que solo los usuarios autorizados puedan acceder a los recursos de la red.

b. Se aplicarán políticas de contraseñas fuertes, la autenticación de dos factores y el cifrado de datos para garantizar la seguridad de las comunicaciones de red.

16.3 Monitoreo y Detección de Intrusiones

a. Se implementarán sistemas de monitoreo y detección de intrusiones para identificar y responder rápidamente a posibles actividades maliciosas en la red.

b. Se establecerán alertas y registros de auditoría para registrar y analizar los eventos de seguridad de la red y tomar medidas correctivas apropiadas.

16.4 Protección contra *Malware* y Amenazas Web

a. Se utilizarán soluciones de seguridad actualizadas, como antivirus y sistemas de filtrado web, para proteger la red contra *malware* y amenazas web.

b. Se implementarán políticas de navegación segura y se educará a los usuarios sobre las mejores prácticas para evitar la descarga o ejecución de archivos maliciosos desde la red.

16.5 Actualizaciones y Parches de Seguridad

a. Se establecerá un proceso de gestión de parches y actualizaciones para mantener al día los sistemas y dispositivos de red, corrigiendo las vulnerabilidades conocidas y mejorando la seguridad de la red.

b. Se realizarán evaluaciones de riesgos y pruebas de compatibilidad antes de aplicar las actualizaciones, asegurándose de minimizar los impactos en la disponibilidad y el rendimiento de la red.

16.6 Respaldo y Recuperación de la Red

a. Se realizarán copias de seguridad regulares de la configuración de red y se establecerá un plan de recuperación de desastres para garantizar la disponibilidad y la continuidad de la red en caso de fallos o incidentes.

b. Se probará periódicamente la capacidad de recuperación de la red y se actualizarán los planes según sea necesario.

17. Seguridad de los servicios de red

Objetivo: garantizar la seguridad en el uso de los servicios de red.

17.1 Autenticación y Autorización de Usuarios

a. Se implementarán mecanismos de autenticación sólidos para verificar la identidad de los usuarios antes de otorgarles acceso a los servicios de red.

b. Se establecerán procedimientos de autorización para asignar privilegios y permisos adecuados a los usuarios, asegurándose de que solo tengan acceso a los recursos y servicios necesarios.

17.2 Encriptación de Datos

a. Se utilizará el cifrado de datos para proteger la confidencialidad de la información transmitida a través de los servicios de red, evitando la interceptación no autorizada.

b. Se implementarán protocolos seguros, como HTTPS, para garantizar la seguridad de las comunicaciones en línea.

17.3 Control de Acceso a los Servicios

a. Se establecerán procedimientos de control de acceso para restringir el acceso a los servicios de red solo a usuarios autorizados.

b. Se implementarán medidas como *firewalls*, listas de control de acceso y sistemas de detección y prevención de intrusiones para proteger los servicios de red contra accesos no autorizados y ataques.

17.4 Monitoreo y Registro de Actividades

a. Se realizará un monitoreo continuo de las actividades en los servicios de red para detectar comportamientos anómalos o actividades sospechosas.

b. Se registrarán y analizarán los eventos de seguridad relacionados con los servicios de red, proporcionando una evidencia crucial para la investigación de incidentes y la respuesta a posibles ataques.

17.5 Actualizaciones y Parches de Seguridad

a. Se mantendrán actualizados los servicios de red con las últimas actualizaciones y parches de seguridad para mitigar las vulnerabilidades conocidas.

b. Se realizarán pruebas y evaluaciones de seguridad antes de implementar las actualizaciones para minimizar los impactos en la disponibilidad y el rendimiento de los servicios.

17.6 Respaldo y Recuperación de los Servicios

a. Se realizarán copias de seguridad periódicas de los datos y configuraciones de los servicios de red, asegurando la disponibilidad de información y la rápida recuperación en caso de fallos o desastres.

b. Se establecerá un plan de recuperación de desastres para restaurar los servicios de red en el menor tiempo posible y minimizar la interrupción para los usuarios.

18. Segregación de redes

Objetivo: dividir la red en límites de seguridad y controlar el tráfico entre ellos en función de las necesidades comerciales.

18.1 Segmentación de Redes

a. Se dividirá la red en segmentos o subredes lógicas basadas en las necesidades comerciales y la sensibilidad de los datos, estableciendo límites de seguridad claros.

b. Se utilizarán *firewalls* y dispositivos de red para separar los segmentos de red y controlar el tráfico entre ellos.

18.2 Políticas de Acceso y Control

a. Se establecerán políticas de acceso y control para regular el tráfico entre los segmentos de red, asegurando que solo el tráfico autorizado pueda cruzar los límites establecidos.

b. Se implementarán mecanismos de autenticación y autorización para garantizar que los usuarios y dispositivos solo accedan a los segmentos de red correspondientes a sus necesidades y privilegios.

18.3 Inspección de Tráfico y Monitoreo

a. Se realizará una inspección continua del tráfico de red para detectar y prevenir posibles amenazas y actividades maliciosas que intenten cruzar los límites de seguridad establecidos.

b. Se utilizarán herramientas de monitoreo de red para identificar patrones anómalos de tráfico y responder rápidamente a posibles incidentes de seguridad.

18.4 Separación de Ambientes

a. Se establecerán segmentos de red específicos para diferentes entornos, como producción, desarrollo y pruebas, asegurando la separación y protección de los datos sensibles y la continuidad operativa.

b. Se aplicarán controles de acceso estrictos para restringir la comunicación entre los ambientes y prevenir la propagación de amenazas o errores entre ellos.

18.5 Gestión Centralizada de la Seguridad

a. Se implementará una solución centralizada de gestión de seguridad de red para facilitar la configuración, supervisión y aplicación consistente de las políticas de segregación de redes.

b. Se realizarán revisiones periódicas de la configuración y ajustes necesarios para mantener la efectividad de la segregación de redes y adaptarla a los cambios en las necesidades comerciales.

19. Separación de los entornos de desarrollo, prueba y producción

Objetivo: proteger el entorno de producción y los datos contra el compromiso de las actividades de desarrollo y prueba.

19.1 Segregación física de los entornos

a. Se establecerán áreas físicas separadas para los entornos de desarrollo, prueba y producción, evitando la interconexión directa y asegurando la protección de los datos sensibles en el entorno de producción.

b. Se implementarán medidas de seguridad física, como el control de acceso y la vigilancia, para prevenir el acceso no autorizado a los entornos de producción.

19.2 Segregación lógica de los entornos

a. Se utilizarán técnicas de virtualización o contenedores para crear instancias separadas de los entornos de desarrollo, prueba y producción, garantizando una separación lógica adecuada y evitando la interferencia entre ellos.

b. Se aplicarán controles de acceso y autenticación para garantizar que solo los usuarios autorizados tengan acceso a cada entorno, reduciendo el riesgo de compromiso accidental o malicioso.

19.3 Control de cambios y gestión de versiones

a. Se establecerá un proceso de control estricto de cambios y gestión de versiones para los entornos de desarrollo y prueba, asegurando que solo los cambios aprobados y probados se implementen en el entorno de producción.

b. Se mantendrá un registro de todos los cambios realizados en los entornos de desarrollo y prueba, proporcionando una trazabilidad completa y permitiendo la identificación rápida de cualquier cambio no autorizado o inesperado.

19.4 Privilegios y accesos diferenciados

a. Se asignarán roles y permisos específicos a los usuarios de cada entorno, limitando el acceso a funciones y datos según las necesidades comerciales y las responsabilidades de cada individuo.

b. Se implementarán controles de acceso, basados en políticas para garantizar que los usuarios solo tengan acceso a los recursos y datos necesarios para realizar sus tareas en cada entorno.

19.5 Auditorías y monitoreo

a. Se realizarán auditorías periódicas para verificar el cumplimiento de las políticas de separación de entornos y detectar posibles desviaciones o violaciones.

b. Se establecerán sistemas de monitoreo y detección de anomalías para identificar cualquier actividad sospechosa o intentos de acceso no autorizados a los entornos de producción desde los entornos de desarrollo o prueba.

20. Gestión de cambios

Objetivo: preservar la seguridad de la información al ejecutar cambios.

20.1 Evaluación y aprobación de cambios

a. Se establecerá un proceso formal para evaluar y aprobar los cambios propuestos antes de su implementación.

b. Se realizará una evaluación de impacto y riesgo para determinar los posibles efectos en la seguridad de la información y tomar las medidas necesarias para mitigar los riesgos identificados.

20.2 Control de versiones y documentación

a. Se utilizará un sistema de control de versiones para gestionar y rastrear los cambios realizados en los sistemas, aplicaciones y servicios.

b. Se mantendrá una documentación precisa de los cambios realizados, incluyendo detalles como el autor, la fecha, la descripción y el motivo del cambio.

20.3 Pruebas y validación

a. Antes de implementar un cambio, se realizarán pruebas exhaustivas para verificar su funcionamiento correcto y su compatibilidad con la infraestructura existente.

b. Se establecerá un proceso de validación para confirmar que el cambio cumple con los requisitos y no afecta negativamente la seguridad de la información.

20.4 Segregación de entornos de desarrollo y producción

a. Se mantendrán entornos separados para el desarrollo y la producción, evitando la ejecución de cambios directamente en el entorno de producción.

b. Los cambios se implementarán primero en un entorno de desarrollo o prueba y luego se migrarán al entorno de producción después de una revisión y aprobación adecuadas.

20.5 Gestión de cambios emergentes

a. Se establecerá un proceso específico para gestionar los cambios emergentes que requieran una implementación inmediata debido a problemas de seguridad o de otro tipo.

b. Los cambios emergentes se evaluarán, aprobarán y documentarán de manera adecuada, garantizando que se sigan los procedimientos de seguridad establecidos.

20.6 Comunicación y entrenamiento

a. Se comunicarán los cambios planificados a las partes interesadas pertinentes y se proporcionará capacitación adecuada sobre los procedimientos y las implicaciones de los cambios.

b. Se promoverá la conciencia y la comprensión de los cambios entre los usuarios y se brindará soporte adicional en caso necesario.

21. Filtrado web

Objetivo: proteger los sistemas contra el *malware* y evitar el acceso a sitios web no autorizados.

21.1 Acceso a sitios web

a. Se implementará un filtro web que controle y restrinja el acceso a sitios web no autorizados desde los sistemas de la organización.

b. Se establecerá una lista de sitios web permitidos y bloqueados, basada en las necesidades de la organización y las políticas de seguridad.

21.2 Bloqueo de contenido malicioso

a. Se configurará el filtro web para bloquear el acceso a sitios web conocidos por distribuir *malware*, *phishing* u otro contenido malicioso.

b. Se realizará una actualización regular de las listas de sitios web maliciosos para mantener la efectividad del filtro y proteger los sistemas contra amenazas conocidas.

21.3 Análisis de contenido

a. El filtro web realizará análisis de contenido en tiempo real para identificar y bloquear sitios web que contengan *malware*, virus u otro contenido dañino.

b. Se establecerá una configuración adecuada para garantizar una detección precisa y una respuesta rápida a las amenazas identificadas.

21.4 Protección contra descargas no autorizadas

a. Se configurará el filtro web para bloquear la descarga de archivos de sitios web no autorizados o de aquellos que presenten un alto riesgo de contener *malware*.

b. Se establecerán políticas claras sobre qué tipos de archivos pueden ser descargados y desde qué fuentes confiables.

21.5 Supervisión y registro

a. Se implementará un sistema de supervisión y registro para rastrear y auditar el acceso a sitios web, incluyendo los intentos de acceso a sitios bloqueados.

b. Los registros se revisarán regularmente para detectar posibles actividades sospechosas o violaciones de las políticas de acceso a sitios web.

21.6 Educación y concientización

a. Se proporcionará capacitación regular a los empleados sobre los riesgos asociados con el acceso a sitios web no autorizados y la importancia de seguir las políticas de filtrado web.

b. Se fomentará una cultura de seguridad informática, alentando a los empleados a informar cualquier actividad sospechosa o intentos de acceso a sitios web bloqueados.

Referencias

ISO/IEC. (2022). ISO/IEC 27002:2022 Tecnología de la información — Técnicas de seguridad — Código de práctica para los controles de seguridad de la información.

Control de cambios

Control de cambios y versiones				
Versión	Fecha de versión	Motivo de la actualización	Nombre del encargado(s)	Firma
01	14-04-2023	Creación de las políticas de seguridad físicas.	William García Molina Michelle Rodríguez Hernández	

Anexo 9: Carta de recibido de la empresa

Distribuidora coarsa
distribución y mercadeo de calidad

San Ramón, 18 de agosto del 2023

Señores

Universidad Técnica Nacional

Sede del Pacífico

Me dirijo a ustedes con el propósito de informarles que los estudiantes **William García Molina (cédula 6-0436-0917)** y **Michelle Rodríguez Hernández (cédula 6-0455-0898)**, quienes cursan la carrera de Licenciatura en Ingeniería en Tecnologías de Información en esta prestigiosa institución que ustedes representan, han presentado los documentos titulados **"Políticas de Seguridad Físicas"** y **"Políticas de Seguridad Tecnológicas"**. Estos documentos son el resultado final del proyecto de graduación denominado**"Analizar los controles para la seguridad de la información implementados por la empresa Distribuidora COARSA, en San Ramón de Alajuela, de acuerdo con la norma ISO 27002, durante el segundo semestre del año 2022".**

Me complace informarles que los estudiantes han finalizado exitosamente este proyecto después de meses de arduo trabajo. Los documentos entregados reflejan un análisis exhaustivo y detallado de los controles de seguridad implementados por la empresa, cumpliendo con los estándares establecidos por la **norma ISO 27002:2022**.

Agradezco su colaboración y aprovecho la oportunidad para expresar mi total disposición a brindar cualquier información adicional que puedan requerir.

ATENTAMENTE

208110152.

Kimberly Montoya

Departamento de TI

coarsa@coarsacr.com● San Ramón, Alajuela● Tel. 2447-1959 ● Fax. 2447-1959

Anexo 10: Carta de solicitud de limitación de permisos de publicación

Distribuidora coarsa

San Ramón, 18 de agosto del 2023

Señores

Universidad Técnica Nacional

Sede del Pacífico

Me dirijo a ustedes con el propósito de informarles que luego de revisar los documentos titulados **"Políticas de Seguridad Físicas"** y **"Políticas de Seguridad Tecnológicas"**. Los cuales son el resultado final del proyecto de graduación denominado**"Analizar los controles para la seguridad de la información implementados por la empresa Distribuidora COARSA, en San Ramón de Alajuela, de acuerdo con la norma ISO 27002, durante el segundo semestre del año 2022"**. Presentados por los estudiantes **William García Molina (cédula 6-0436-0917)** y **Michelle Rodríguez Hernández (cédula 6-0455-0898)**, quienes cursan la carrera de Licenciatura en Ingeniería en Tecnologías de Información en esta prestigiosa institución que ustedes representan, me he percatado que el proyecto contiene una serie de informacion sensible de la empresa, por lo tanto les solicito respetuosamente, limitar los permisos de uso del trabajo a únicamente los minimos necesarios,en medida de lo posible, que este no sea publicado en internet, lo anterior con el fin de proteger los datos de la organizacion.

Agradezco su colaboración y aprovecho la oportunidad para expresar mi total disposición a brindar cualquier información adicional que puedan requerir.

ATENTAMENTE

Kimberly Montoya

Departamento de TI

coarsa@coarsacr.com • San Ramón, Alajuela • Tel. 2447-1959 • Fax. 2447-1959

Anexo 11: Carta de autorización para uso y manejo

CARTA DE AUTORIZACIÓN PARA USO Y MANEJO DE LOS TRABAJOS FINALES DE GRADUACIÓN
UNIVERSIDAD TÉCNICA NACIONAL
(Trabajo colectivo)

Puntarenas
22 de agosto del 2023
Señores
Vicerrectoría de Investigación
Sistema Integrado de Bibliotecas y Recursos Digitales

Estimados señores:

Nombre de completo de sustentantes	Número de Identificación
William de Jesús García Molina	604360917
Michelle Rodríguez Hernández	604550898

Nosotros en calidad de autores del trabajo de graduación titulado:
Analizar los controles para la seguridad de la información implementados por la empresa Distribuidora COARSA, en San Ramón de Alajuela, de acuerdo con la norma ISO 27002, durante el segundo semestre del año 2022
_____
_____.

El cual se presenta bajo la modalidad de, marque una opción:

_____ Seminario de Graduación

__X__ Proyecto de Graduación

_____ Tesis de Graduación

Presentado en la fecha 12/08/2023, autorizamos a la Universidad Técnica Nacional, Sede del pacifico, para que nuestro trabajo pueda ser manejado de la siguiente manera:

Autorizamos **Ver CAPÍTULO V, DISPOSICIONES, FINALES. Artículo 43. RTFG.**	
Marque con una X o un ✓	
Conservación de ejemplares para préstamo y consulta física en biblioteca	✓
Inclusión en el catálogo digital del SIBIREDI (Cita catalográfica).	X
Comunicación y divulgación a través del Repositorio Institucional	X
Divulgación del resumen en el Repositorio UTN con una cantidad de 200 a 500 palabras.	✓
Consulta electrónica con texto protegido.	X
Descarga electrónica del documento en texto completo protegido.	X
Inclusión en bases de datos y sitios web que se encuentren en convenio con la Universidad Técnica Nacional contando con las mismas condiciones y limitaciones aquí establecidas.	X

Por otra parte, declaramos que el trabajo que aquí presentamos es de plena autoría, es un esfuerzo realizado de forma conjunta, académica e intelectual con plenos elementos de originalidad y creatividad. Garantizamos que no contiene citas, ni transcripciones de forma indebida que puedan devenir en plagio, pues se ha utilizado la normativa vigente de la American Psychological Asociation (APA). Las citas y transcripciones utilizadas se realizan en el marco de respeto a las obras de terceros. La responsabilidad directa en el diseño y presentación son de competencia exclusiva, por tanto, eximo de toda responsabilidad a la Universidad Técnica Nacional.

Conscientes de que las autorizaciones no reprimen nuestros derechos patrimoniales como autores del trabajo. Confiamos en que la Universidad Técnica Nacional respete y haga respetar nuestros derechos de propiedad intelectual

Nombre del estudiante	**Cédula**	**Firma**
William de Jesús García Molina	604360917	William Garcia.
Michelle Rodríguez Hernández	604550898	

Día: 22/08/2023