CENTRO DE POSGRADOS

Tema:

POLÍTICA DE SEGURIDAD INFORMÁTICA PARA *HOLDING* DE EMPRESAS EN BASE A LA NORMA ISO/IEC 27002

Proyecto de investigación previo a la obtención del título de Magister en Ciberseguridad

Línea de investigación:

SEGURIDAD DE LA INFORMACIÓN

Autor:

Darío Alejandro Gutiérrez Jácome

Director:

Mg. Galo Mauricio López Sevilla

Ambato – Ecuador

Marzo 2025

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **DARÍO ALEJANDRO GUTIÉRREZ JÁCOME**, con cédula de ciudadanía **0503164113**, autor del trabajo de graduación intitulado: "POLÍTICA DE SEGURIDAD INFORMÁTICA PARA *HOLDING* DE EMPRESAS EN BASE A LA NORMA ISO/IEC 27002", previa a la obtención del título profesional de **MAGISTER EN CIBERSEGURIDAD**, en el centro de **POSGRADOS**.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, con respeto de las políticas de propiedad intelectual de la Universidad.

Ambato, marzo 2025

Darío Alejandro Gutiérrez Jácome
CC. 0503164113

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

APROBACIÓN DE TRIBUNAL DE GRADO

Tema:

POLÍTICA DE SEGURIDAD INFORMÁTICA PARA *HOLDING* DE EMPRESAS EN BASE A LA NORMA ISO/IEC 27002

Línea de investigación:

SEGURIDAD DE LA INFORMACIÓN

Autor:

Darío Alejandro Gutiérrez Jácome

Galo Mauricio López Sevilla, Ing. Mg. f._____
Firmado electrónicamente por: GALO MAURICIO LOPEZ SEVILLA

CC: 1802836039

CALIFICADOR

Enrique Xavier Garcés Freire, Ing. Mg. f._____
Firmado electrónicamente por: ENRIQUE XAVIER GARCES FREIRE

CALIFICADOR

Darío Javier Robayo Jácome, Ing. Mg. f._____
Firmado electrónicamente por: DARIO JAVIER ROBAYO JACOME

CALIFICADOR

Dayamy Lima Rojas, Lic. Mg. f._____
Firmado electrónicamente por: DAYAMY LIMA ROJAS

DIRECTORA CENTRO DE POSGRADOS

Diego Gonzalo Coca Chanalata, Dr. f._____
DIEGO GONZALO COCA CHANALATA
Firmado digitalmente por DIEGO GONZALO COCA CHANALATA
Fecha: 2025.03.07 08:49:05 -05'00'

SECRETARIO GENERAL PUCESA

Ambato – Ecuador

Marzo 2025

DEDICATORIA

Dedico este proyecto de tesis en primer lugar a Dios por sus bendiciones para realizar el presente proyecto; a mis padres por su apoyo e estimulo incondicional que lo mantuvieron durante desde el comienzo de la carrera y todo el proyecto, a mis hermanos Diego y Yadira los cuales estimo mucho porque me estuvieron incentivando a la culminación de la tesis y la obtención de mi título de grado. A mis amigos que me dieron ese apoyo para la culminación de la tesis.

Lo dedico a mis seres queridos que ya no están, y que desde el cielo me dieron su apoyo incondicional.

Y a todas esas personas que hicieron posible que mi meta se cumpliera.

Darío Gutiérrez

AGRADECIMIENTO

Mi agradecimiento primero a Dios por haberme bendecido para lograr mis objetivos.

A mis padres y hermanos, quienes han sabido escucharme y apoyarme siempre, y en todo momento; muchas gracias por toda una vida de felicidad, amor, comprensión y por estar conmigo en las buenas y malas.

A mis amigos y compañeros de trabajo, por haberme apoyado también en todo momento para la culminación de mis estudios.

A mi Director de tesis que con sus conocimientos me ayudó en todo lo necesario, Mg. Galo Mauricio López Sevilla.

A la Pontificia Universidad Católica del Ecuador por permitirnos realizar nuestro proyecto, preparándonos para un mundo profesional competitivo y lleno de nuevos retos.

Darío Gutiérrez

RESUMEN

En el holding de empresas Ambacar Cía. Ltda., concesionarios de venta de vehículos a nivel nacional, Ciudad del Auto CIAUTO Cía. Ltda. ensambladora de vehículos, se hace necesario el desarrollo de una política de seguridad informática, por el incremento en los últimos años de ataques informáticos como, *Phishing, RANSOMWARE*, entre otros, sobre organizaciones de la industria automotriz, afectando la seguridad de la información.

Es importante realizar este estudio para proteger los activos e información del holding de empresas y mitigar los incidentes en seguridad de la información, evitando costes graves e inesperados, o una grave perturbación de los servicios y actividades comerciales.

Para implementar la política de seguridad informática para el holding de empresas se aplica la metodología descrita Norma ISO/IEC 27002, que tiene como finalidad mitigar posibles vulnerabilidades en los sistemas de información, estableciendo dominios, objetivos y controles para la gestión de la seguridad de la información, usando el tipo de investigación de campo, con enfoque cuantitativo no experimental. Los resultados se sintetizarán en una matriz de riesgos, donde se detallan los activos de información y los riesgos a evaluar.

Luego de realizar el diagnóstico, se llevará a cabo un análisis de la norma internacional ISO/IEC 27002, para identificar controles aplicables y así poder mitigar los eventos de alto riesgo; y como último paso, la aprobación de la política de seguridad informática.

Palabras clave: política informática, ISO/IEC 27002, gestión de la seguridad.

ABSTRACT

In the corporate holding comprising Ambacar Cia. Ltda., a nationwide vehicle dealership, and Ciudad del Auto CIAUTO Cia. Ltda. - a vehicle assembly plant, the development of an information security policy has become imperative due to the increasing frequency of cyberattacks such as phishing and ransomware targeting the automotive industry in recent years. These attacks have compromised the security of the information.

This study aims to protect the assets and information of the corporate holding and mitigate information security incidents, thereby preventing significant and unexpected costs or severe disruptions to business services and activities.

To implement the information security policy for the corporate holding, the methodology described in the ISO/IEC 27002 standard has been applied. This standard aims to mitigate potential vulnerabilities in information systems by establishing domains, objectives, and controls for information security management. A quantitative, non-experimental field research approach was employed. The results will be summarized in a risk matrix, detailing information assets and risks to be assessed.

Following the diagnosis, an analysis of the ISO/IEC 27002 international standard will be conducted to identify applicable controls to mitigate high-risk events. And as a final step, of the international standard ISO/IEC 27002 will be carried out to identify applicable controls to mitigate high-risk events; and as a last step, the approval of the information security policy.

***Keywords**: information security policy, ISO/IEC 27002, security management.*

ÍNDICE GENERAL DE CONTENIDOS

INTRODUCCIÓN

Al presente los sistemas de información, los datos contenidos en ellos y la información son los activos más valiosos para las organizaciones a nivel mundial y se hace necesario establecer una protección adecuada frente a las posibles intrusiones derivadas de las vulnerabilidades existentes en sus sistemas de seguridad. Una de las formas efectiva de descubrir las debilidades y amenazas existentes es iniciando los procesos diagnósticos que permitan medir el estado actual de la seguridad dentro de las organizaciones, teniendo en cuenta las normativas vigentes y los procesos de análisis y evaluación de riesgos, la verificación de la existencia de controles de seguridad existentes, las pruebas con software y el monitoreo de los sistemas de información permiten establecer el estado actual de las organizaciones e identificar las causas de vulnerabilidades y proponer soluciones de control que permitan su mitigación.

En el informe de la Unión Internacional de Comunicaciones (ITU) 2019-2020 en la clasificación de uso de políticas de seguridad sitúa al Ecuador en el puesto 119 a nivel global y en el puesto 19 a nivel de la región americana. Esto de alguna manera evidencia que se necesita trabajar más en el diseño e implementación de políticas de seguridad para mitigar o prevenir ataques, los cuales pueden afectar la estructura de las organizaciones y sus procesos.

El *holding* de empresas Ambacar Cía. Ltda., conformado por concesionarios de venta de vehículos a nivel nacional, Ciudad del Auto CIAUTO Cía. Ltda. ensambladora de vehículos, ubicados en Ambato, tienen implementados parcialmente ciertos procesos relacionados a la seguridad de la información; sin embargo, no tienen documentados herramientas de seguimiento, *firewalls*, controles de ingreso externo por VPN, control de dispositivos por *MAC address* o IP, así como tampoco existe una gestión centralizada de antivirus, ni soluciones para el cambio de contraseñas para servidores y usuarios que ingresan externamente; tampoco se dispone de restricciones para los niveles de información por procesos o por el puesto de trabajo. Así la seguridad de la información no tiene un control correcto aplicado a los usuarios; adicionalmente,

se mantiene parcialmente documentado y organizado los activos del *Holding* de empresas, y no se tiene medido el nivel del riesgo de la información importante que se mantienen en los dispositivos. Por tanto, se ha comprobado que existe fuga o perdida de información, al no tener un control medido del acceso externo a la red interna, ni a los computadores portátiles que se conectan desde fuera de la organización; generando inseguridad en los datos usados y mantenida por los usuarios.

Con la perspectiva anterior surgen las siguientes preguntas. ¿Es importante la identificación de elementos teóricos y metodológicos asociados a normas y estándares a aplicarse en el holding de empresas?, también se deberá considerar, ¿Qué metodología es la más adecuada para la elaboración de un plan con normas y estándares de seguridad informática?, considerando la pregunta anterior, ¿Cuáles son los principales elementos para determinar la composición de pasos organizados del plan de seguridad informática adecuada para el holding de empresas?

Para dar solución a las preguntas planteadas anteriormente se ve la necesidad de, desarrollar una política de seguridad informática para el *Holding* de empresas en base a la Norma ISO/IEC 27002. Para este proceso se tiene como primer paso, la identificación de elementos teóricos y metodológicos relacionados a la norma internacional ISO/IEC 27002 a la par ir realizando la identificación del estado actual de la organización, los riesgos bajos, medios y altos para la revisión de los controles de la norma internacional ISO/IEC 27002. Con los datos recolectados anteriormente se procedió con la elaboración de un plan de contingencia para la mitigación de los riesgos obtenidos de la matriz, con todo lo anterior se hará la presentación de la política de seguridad informática basada en las normas y estándares técnicos de la ISO/IEC 27002.

Para determinar la situación actual de conocimiento de los usuarios y los niveles de seguridad del *holding* de empresas, se hará uso de la investigación de campo, con enfoque cuantitativo no experimental, por tal motivo se usarán herramientas

como listas de chequeo, encuestas, matriz de riesgos, para el proceso de desarrollo se hará uso de la norma ISO/IEC 27002.

El objetivo de desarrollar una política de seguridad informática para el *Holding* de empresas, es acoger un documento actualizado y efectivo que contemple normas internacionales de seguridad de información. Por esta razón una de las mejores opciones adaptable a las necesidades es la norma ISO/IEC 27002, porque que mediante sus dominios y controles se puede establecer un adecuado control y revisión de los incidentes de seguridad que ocurren dentro de las organizaciones.

Con la revisión y análisis de la norma internacional ISO/EC 27002, se pudo implementar controles de seguridad de la información y poder mitigar los eventos de riego que mantiene las organizaciones, inclusive se puede establecer buenas prácticas de seguridad informática para los diferentes niveles de los procesos y la concientización de los empleados.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Estado de arte

La norma ISO 27002 es conocida en la informática por ser un estándar que se destaca en las organizaciones. Actualmente, concurren varios estudios relacionados sobre el tema a nivel nacional e internacional. (Cevallos Jarro, s. f.) diseñó una política de seguridad de la información para el área de TI del Instituto Tecnológico Superior Central Técnico, mediante la aplicación de la norma de seguridad ISO/IEC 27002: 2013.

Asimismo, Contero (2019), en el marco de su tesis de maestría en la UISEK realizó el diseño de una política de seguridad de la información, usando la norma ISO 27002:2013 para el sistema de botones de seguridad del Ministerio del Interior.

Al igual que (Guallpa Zatán, s. f.) en su tesis de maestría, realizó un plan de seguridad informática basado en la ISO 27002, para el control de accesos indebidos a la red de la Uniandes (sede Puyo), donde se detalla controles de accesos en las áreas catalogadas críticas, lo que muestra una visión mucho más amplia de lo que se debe implementar, así como de las capacitaciones a llevar adelante con las personas responsables de los procesos involucrados.

La seguridad informática de cierta manera no tiene la atención necesaria y al no ser implementada se pierden medidas de protección y procesos de mitigación, de tal modo que las organizaciones quedan expuestas y vulnerables, por lo que sufrirían complicaciones serias en la integridad de los activos y aseguramiento de la información.

Una vez realizado el análisis de los artículos citados, se puede concluir que: la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT), es la opción más efectiva y completa para el análisis, elaboración de matriz de riesgos en el área de la informática, permite dar un valor a los activos en

base a su integridad, disponibilidad y confidencialidad, como también ayuda a la identificación de amenazas y vulnerabilidades que pueden afectar los activos, facilitando la elección de medidas de seguridad y garantizando el éxito en cada uno de los procesos; y, para la selección y elaboración de las normas, medidas de seguridad, se tomará como referencia la Norma ISO/IEC 27002, porque puede ser implementada en empresas pequeñas como en grandes organizaciones, públicas o privadas garantizando la confidencialidad, integridad y disponibilidad de la información.

1.2. Seguridad informática

La seguridad informática se muestra como las acciones tácticas y operacionales de la seguridad.

La seguridad informática en la actualidad es un tema central para todos los usuarios de equipos de cómputo, ya sean de escritorio o móviles, en el hogar, en la escuela o dentro de una organización. Esto entorno al uso del Internet en auge conlleva importantes riesgos de seguridad. El Internet es usado para propósitos para los cuales no fue concebido desde su creación. Inicialmente el Internet fue diseñado para promover la conectividad y no la seguridad (Roque Hernández & Juárez Ibarra, 2018).

Para ISOTools Excellece la seguridad informática (*IT security*), es el método que se encarga de realizar las diferentes soluciones técnicas de protección de la información. "La seguridad informática protege el sistema informático, tratando de asegurar la integridad y la privacidad de la información que contiene. Por lo tanto, podríamos decir, que se trata de implementar medidas técnicas que preservarán las infraestructuras y de comunicación que soportan la operación de una empresa, es decir, el hardware y el software empleados por la empresa" (ISOTools Excellence, s. f.).

Los Consultores en Seguridad de la Información mencionan que la seguridad informática o igualmente llamada seguridad de tecnologías de la información, la

definen como "el área de la informática que consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización, sean utilizados de manera correcta" (*CSI Consultores en Seguridad de la Información*, s. f.).

Dado lo anterior, plantea que la Seguridad Informática, es la "disciplina que se encargaría de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que-articulados con prácticas de gobierno de tecnología de información-establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo" (Figueroa-Suárez et al., 2018).

Además, se indica que la seguridad informática es un conjunto de métodos, procesos y/o técnicas que tiene como objetivo la protección de los sistemas informáticos y la información en formato digital que éstos almacenen. Y alude que "Dentro de esta categoría, se puede mencionar la seguridad computacional, la cual se ciñe a la protección de los sistemas y equipos para el procesamiento de datos” (Enríquez et al., 2022).

De lo citado anteriormente se puede concluir que la seguridad informática conlleva la protección de la información con diferentes métodos y herramientas cuyo objetivo es precautelar, controlar, mantener la integridad de los diferentes activos y datos mantenidos por las organizaciones y los usuarios.

Términos y problemas de la seguridad informática

Hackers y crackers

(Richet, 2013) menciona que, un hacker es una persona con alto nivel de conocimientos y técnicas que utiliza una computadora para tener acceso a un equipo o red, con el objetivo de realizar actividades no autorizadas. Varios

expertos argumentan que los hackers trabajan con principios éticos y que sus acciones no llevan una intención maliciosa. Por el contrario, un cracker, aunque posee conocimientos similares tiene unos objetivos maliciosos implícitos en su conducta.

Desde que se creó el termino Hacker se lo ha malinterpretado, porque un hacker es aquel que trabaja con conocimientos y principios éticos y en pro de mejorar la seguridad en los sistemas y redes. Mientras que los crackers tienen un amplio conocimiento, pero sus acciones son mal intencionadas, de forma de lucrar u simplemente hacer daño.

Gusanos, troyanos y *SPYWARE*

El código malicioso es cualquier programa desarrollado para producir inconvenientes al usuario (*Gestión de vulnerabilidades*, 2024). Sus acciones pueden incluir destrucción de datos, uso de recursos con fines malintencionados y robo de información. Gusanos, troyanos y *SPYWARE* son ejemplos de este tipo de código.

(*Recognizing and Avoiding Spyware* | *CISA*, 2009) describen a los gusanos como programas maliciosos que se pueden replicar a sí mismos dentro un dispositivo o red, y se pueden ser enviados desde distintos lugares por ejemplo en internet a través de mensajería instantánea, o en redes para compartir archivos. Varios de los gusanos son ampliamente conocidos por los usuarios siguen teniendo éxito en sus infecciones, en la actualidad hay brechas y vulnerabilidades de seguridad de los sistemas actuales.

Los troyanos son programas que no se replican a sí mismos, traen consigo un paquete de diferentes tipos de gusanos, pero se puede presentar al usuario de varias maneras por ejemplo una funcionalidad aparentemente útil como la de eliminar virus en su sistema. Una vez ejecutados estos programas infectan el equipo, dispositivos con virus que pueden enviar información, brindar acceso remoto o deshabilitar opciones de protección. Los troyanos son difíciles de

detectar, porque vienen enmascarados como una utilidad para el usuario, pero es justamente lo opuesto y ralentizan las operaciones de la computadora.

El término *SPYWARE* se refiere a los programas que recogen información del usuario sin su conocimiento. Dichos programas pueden ser usados para mostrar contenidos que puede ser relevante para el usuario o bien para instalar otros programas que pueden guardar información de las teclas oprimidas (*KEYLOGERS)* y de esta manera robar contraseñas o registrar el historial de búsquedas. El spyware no intenta replicarse a otras computadoras.

PHISHING

Es una manera de adquirir información de forma fraudulenta a través de correo electrónico, estafas, anuncios que parece provenir de una organización legítima (Li et al., 2014). El correo puede incluir documentos adjuntos con virus y otras amenazas, enlaces que conduce a un falso sitio, el cual es una copia del original y se encarga de engañar al usuario para robar contraseñas, información personal o de tarjetas de crédito.

Hasta hace algunos años la identificación de este tipo de amenazas era más sencilla, contenían elementos que visiblemente resultaban sospechosos. Por ejemplo, su diseño era rústico o su redacción era deficiente. Al día de hoy se hace más difícil identificar si un correo es legítimo o no, pues las herramientas maliciosas actuales hacen que la calidad de las falsificaciones haya incrementado notablemente.

Respaldos de información

La información es uno de los activos más importantes para las empresas y para los usuarios (Rhodes-Ousley, s. f.), por lo cual se hace necesario asegurarla; una manera de hacerlo es a través de respaldos (*BACKUPS*). Un respaldo es una copia completa o parcial de los archivos importantes de un sistema informático

que se realiza con la finalidad de prevenir la posible pérdida debido a errores de hardware, software o infecciones de virus estas son algunas causas.

Los respaldos pueden ser completos, es decir, de todos los archivos, o bien incrementales y también parciales. Solo de los archivos que han sido modificados desde el último respaldo; la decisión de realizar un respaldo completo o incremental puede acelerar o disminuir considerablemente el proceso de copia de los archivos (Rhodes-Ousley, s. f.).

Los respaldos deben realizarse de manera periódica y almacenarse en varios sitios distintos donde radica el equipo de cómputo y dispositivos para prevenir la pérdida por desastre físico. De esta manera, el almacenamiento en la nube es una buena opción para guardar los respaldos, pues sus servidores se encuentran geográficamente distantes del equipo que está siendo respaldado.

1.3. Políticas de seguridad en las organizaciones

En consideración al desarrollo de las políticas de seguridad informática para las organizaciones, se tomará en cuenta el siguiente criterio:

Lo primero que deben hacer es un análisis de las posibles amenazas que puede llegar a sufrir el sistema informático, una estimación de las pérdidas que esas amenazas podrían suponer y un estudio de las probabilidades de que ocurran.

A partir del análisis realizado se deberá diseñar una política de seguridad en la cual se establezcan las responsabilidades y reglas a seguir para evitar esas amenazas o minimizar los efectos si se llegan a producir. (Yupanqui et al., 2017).

Gráfico 1. Política de seguridad

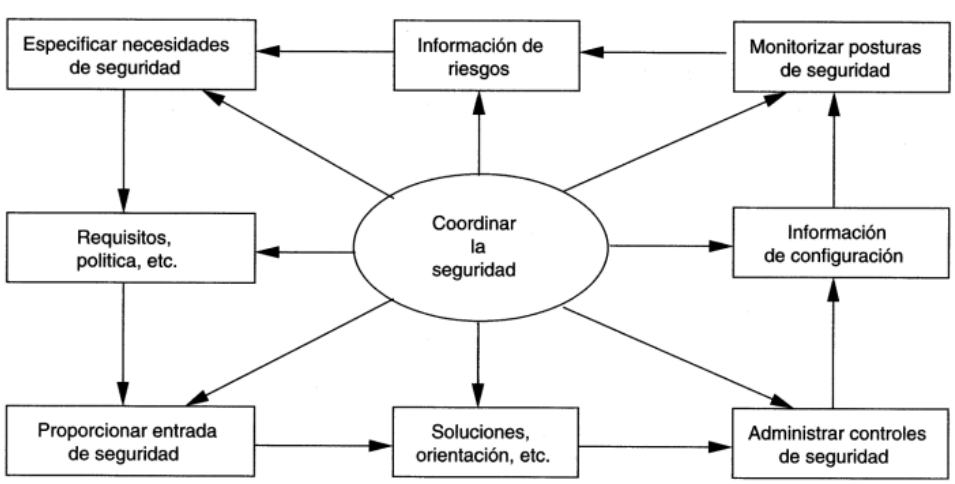
Fuente: Mifsud, E. (2012).

La seguridad informática, de igual manera a como es aplicada a otros entornos, trata de mitigar y prevenir los riesgos asociados al acceso y utilización de determinados sistemas de forma no autorizada y en general malintencionada; como se muestra en el grafico 1 la estructura funcional que debe mantener una política de seguridad.

Objetivo de la seguridad informática en las organizaciones

El objetivo de la seguridad informática es proteger los recursos informáticos valiosos de la organización, tales como información, hardware o software. A través de la aceptación de las medidas adecuadas, la seguridad informática ayuda a una organización a cumplir sus objetivos, permite proteger y asegurar los recursos financieros, sistemas de información, reputación, situación legal, y otros bienes tanto tangibles e intangibles.

Gráfico 2. Objetivo principal de las políticas de seguridad informática



Fuente: (Figueroa-Suárez et al., 2018)

En consecuencia, gestionar la seguridad informática organizacional es una tarea exigente y evaluar periódicamente las tecnologías de seguridad es esencial para mantener una gestión eficaz en la seguridad de la información.

Importancia de las políticas de seguridad informática

La Tecnología de la Información (TI) se está extendiendo constantemente en varias áreas en las organizaciones y es un factor crítico para tener éxito en la economía mundial.

La pérdida, manipulación, divulgación, o la falta de disponibilidad de información causada por incidentes o accidentes en la seguridad de la misma, pueden dar lugar a gastos, pérdida de beneficios o inclusive consecuencias legales. Los diferentes incidentes en la seguridad de la información pueden ser originados por otros actores y diferentes motivos. *Hackers*, profesionales, aficionados, empleados maliciosos, espías industriales, o inclusive terroristas, tratan de introducirse en los sistemas para obtener acceso a la información, solicitar recompensas o simplemente para hacer daño.

Estas personas buscan vulnerabilidades y utilizan cualquier debilidad hallada en la cadena de seguridad de una organización. En la constante lucha que permite que los sistemas de información sean más seguros, las organizaciones siempre están tratando de encontrar nuevas formas de abordar adecuadamente las cuestiones de seguridad.

Es necesario recalcar sobre la importancia que tienen las políticas de seguridad de la información y su debida aplicación en instituciones de abundante procesamiento de información.

Antes de implementar y distribuir la política de seguridad a todos los empleados, debe revisarse para no dejar ninguna brecha legal. Además, hay que asegurarse que la política es clara, concisa y consistente.

También es importante establecer de forma firme la validez de la política de seguridad, que debe observar las leyes establecidas por ésta, para evitar complicaciones legales.

Para que una organización mantenga un nivel suficiente de seguridad, su política de seguridad de la información debe evolucionar para la detección de nuevos tipos de amenazas, para lo que debe revisarse constantemente. De lo contrario, la política dejaría de ser útil (Figueroa-Suárez et al., 2018).

Las políticas de seguridad de la información tienen su guía o complemento en los estándares o normas de seguridad.

En la actualidad se menciona frecuentemente los estándares y normas de seguridad, y es así que se toma en cuenta que:

Un estándar es un documento con un contenido de tipo técnico-legal establece un modelo o norma que refiriere lineamientos, instrucciones a seguir para cumplir una actividad o procedimientos. Su uso se ha popularizado en la actualidad

debido a que se busca que los procesos y actividades de las organizaciones y sus usuarios sean repetibles, organizados, y estructurados (Casa et al., 2021).

Normas de seguridad

Regla de procedimiento dictada por una autoridad competente que se debe seguir o ajustar a las conductas, tareas, actividades, entre otros.

Es por lo cual que, en el *Holding* de empresas, pueden aplicar este tipo de normas de seguridad, con el propósito de precautelar la información que se procesa y que se pone a disposición de la sociedad. Se puede mencionar el conjunto de normas de seguridad de la serie ISO/IEC 27000 resumidas en la siguiente tabla:

Tabla N 1: Conjunto de normas de seguridad de la serie ISO/IEC 27000

Series	Detalles
ISO/IEC 27000	Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación.
ISO/IEC 27001	Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información.
ISO/IEC 27002	Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.
ISO/IEC 27003	No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001.
ISO/IEC 27004	No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.
ISO/IEC 27005	No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información.
ISO/IEC 27006	Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información los requisitos específicos relacionados con ISO 27001:2005 y los SGSIs.
ISO/IEC 27007	Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011.
ISO/IEC TS 27008	No certificable. Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.
ISO/IEC 27009	No certificable. define los requisitos para el uso de la norma ISO/IEC 27001 en cualquier sector específico (campo, área de aplicación o sector industrial).
ISO/IEC 27010	Consiste en una guía para la gestión de la seguridad de la

	información cuando se comparte entre organizaciones o sectores. ISO/IEC 27010:2012 es aplicable a todas las formas de intercambio y difusión de información sensible, tanto públicas como privadas, a nivel nacional e internacional, dentro de la misma industria o sector de mercado o entre sectores.
ISO/IEC 27011	Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002.
ISO/IEC 27013	Es una guía de implementación integrada de ISO/IEC 27001:2013 (gestión de seguridad de la información) y de ISO/IEC 20000-1:2018 (gestión de servicios TI).
ISO/IEC 27014	Consiste en una guía de gobierno corporativo de la seguridad de la información, la ciberseguridad y privacidad.
ISO/IEC TR 27015	Es una guía de SGSI orientada a organizaciones del sector financiero y de seguros y como complemento a ISO/IEC 27002:2005.
ISO/IEC TR 27016	Es una guía de valoración de los aspectos financieros de la seguridad de la información.
ISO/IEC 27017	Es una guía de seguridad para Cloud Computing alineada con ISO/IEC 27002 y con controles adicionales específicos de estos entornos de nube.
ISO/IEC 27018	Es un código de buenas prácticas en controles de protección de datos para aquellos proveedores de servicios de computación en cloud computing.
ISO/IEC TR 27019	Guía con referencia a ISO/IEC 27002:2005 para el proceso de sistemas de control específicos relacionados con el sector de la industria de la energía.
ISO/IEC 27021	Especifica los requisitos de competencia para aquellos profesionales que lideran o participan en el establecimiento, implementación, mantenimiento y mejora continua de uno o más procesos del sistema de gestión de seguridad de la información (SGSI) que cumplan con ISO/IEC 27001.
ISO/IEC 27022	define un modelo de referencia de procesos para el dominio de la gestión de seguridad de la información con el objetivo de guiar a los usuarios de ISO/IEC 27001 a incorporar el enfoque de proceso tal y como se describe en ISO/IEC 27000:2018
ISO/IEC TR 27023	Es una guía de correspondencias entre las versiones del 2013 de las normas ISO/IEC 27001 y ISO/IEC 27002 como apoyo a la transición de las versiones publicadas en 2005.
ISO/IEC 27030	En fase de desarrollo cubrirá la seguridad y privacidad en principios, riesgos y controles aplicables al Internet de las Cosas (IoT - Internet of Things).
ISO/IEC 27031	No certificable. Es una guía de apoyo para la adecuación de las tecnologías de información y comunicación (TIC) de una organización para la continuidad del negocio. El documento toma como referencia el estándar BS 25777.
ISO/IEC 27032	Proporciona orientación para la mejora del estado de seguridad cibernética, extrayendo los aspectos únicos de esa actividad y de sus dependencias en otros dominios de seguridad, concretamente: Información de seguridad, seguridad de las redes, seguridad en Internet e información de protección de infraestructuras críticas (CIIP).
ISO/IEC 27033	Parcialmente desarrollada. Norma dedicada a la seguridad en redes, consistente en 6 partes: 27033-1, conceptos generales directrices de diseño e implementación de seguridad en redes.

ISO/IEC 27034	Parcialmente desarrollada. Norma dedicada la seguridad en aplicaciones informáticas, consistente en 7 partes: conceptos generales, marco normativo de la organización, proceso de gestión de seguridad en aplicaciones, validación de la seguridad en aplicaciones, estructura de datos y protocolos y controles de seguridad de aplicaciones, guía de seguridad para aplicaciones de uso, marco predictivo de en la seguridad.
ISO/IEC 27035	Proporciona una guía sobre la gestión de incidentes de seguridad en la información
ISO/IEC 27036	Guía en cuatro partes de seguridad en las relaciones con proveedores: visión general y conceptos, requisitos comunes, seguridad en la cadena de suministro TIC, guía de seguridad para entornos de servicios Cloud.
ISO/IEC 27037	Es una guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositivos y para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones.
ISO/IEC 27038	Es una guía de especificación para seguridad en la redacción digital.
ISO/IEC 27039	Es una guía para la selección, despliegue y operativa de sistemas de detección y prevención de intrusión (IDS/IPS).
ISO/IEC 27040	Es una guía para la seguridad en medios de almacenamiento.
ISO/IEC 27041	Es una guía para la garantizar la idoneidad y adecuación de los métodos de investigación.
ISO/IEC 27042	Es una guía con directrices para el análisis e interpretación de las evidencias digitales.
ISO/IEC 27043	Desarrolla principios y procesos de investigación para la recopilación de evidencias digitales.
ISO/IEC 27045	En fase de desarrollo, el proyecto se inició en 2018 y cubrirá procesos de seguridad y privacidad en sistemas de big data.
ISO/IEC 27050	Norma desarrollada en tres partes sobre la información almacenada en dispositivos electrónicos en relación a su identificación, preservación, recolección, procesamiento, revisión, análisis y producción
ISO/IEC 27070	Establece requisitos de seguridad para establecer raíces de confianza para la provisión de entornos informáticos confiables, donde las máquinas virtuales se crean dinámicamente para proporcionar servicios en la nube.
ISO/IEC 27071	En fase de desarrollo, recomendará controles de seguridad para establecer conexiones confiables entre dispositivos y servicios en la nube.

Fuente: ISO 27000 (sf). Recuperado de: https://www.iso27000.es/iso27000.html

1.4. ISO/IEC 27002

Antecedentes y contexto

Esta norma internacional está diseñada para que las organizaciones la usen como referencia a la hora de seleccionar controles dentro del proceso de implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la Norma ISO/IEC 27001[10] o bien como documento guía para organizaciones que implanten controles de seguridad de la información comúnmente aceptados. Esta norma está pensada también para usarse en el desarrollo de directrices de gestión de la seguridad de la información en industrias y organizaciones específicas, teniendo en cuenta su(s) entorno(s) específico(s) de riesgo de seguridad de la información (ISO/IEC 27002:2013).

Se establece la Norma ISO/IEC 27002 como una referencia para toda organización donde se requieran la implementación de controles, directrices, para la seguridad de la información y sus activos.

Organizaciones de todo tipo y tamaño (incluyendo sector público y privado, comercial y sin ánimo de lucro) recogen, procesan, almacenan y transmiten información de muchas formas incluyendo medios electrónicos, físicos y verbales (por ejemplo, conversaciones y presentaciones) (ISO/IEC 27002:2013).

El valor de la información trasciende las palabras escritas, los números y las imágenes: el conocimiento, los conceptos, ideas y marcas son ejemplos de formas intangibles de información. En un mundo interconectado, la información y sus procesos relacionados, los sistemas, las redes y el personal implicados en su operación, manejo y protección son activos que, al igual que otros activos importantes del negocio, resultan valiosos para el negocio de una organización y, en consecuencia, merecen o requieren protección contra diversos peligros (ISO/IEC 27002:2013).

Los activos están sujetos tanto a amenazas deliberadas como accidentales, mientras que los procesos relacionados, los sistemas, las redes y las personas tienen vulnerabilidades inherentes. Los cambios en los procesos y sistemas de negocio u otros cambios externos (por ejemplo, nuevas leyes y regulaciones) pueden crear nuevos riesgos relativos a la seguridad de la información. Por lo tanto, dada la multitud de formas en que las amenazas podrían aprovecharse de las vulnerabilidades para dañar a la organización, los riesgos de seguridad de la información están siempre presentes. Una seguridad de la información eficaz reduce estos riesgos protegiendo a la organización frente a las amenazas y vulnerabilidades, y en consecuencia reduce el impacto en sus activos (ISO/IEC 27002:2013).

Toda organización está sujeta a cambios en varios aspectos, por lo cual se crean amenazas y vulnerabilidades en los sistemas de información y también hacia los activos, por lo cual es necesario implantar buenas prácticas y políticas para reducir el riesgo y el impacto en aquellos que es importante, sin importar el tipo de organización en el que este confirmada.

Requisitos de seguridad de la información

Según la (ISO/IEC 27002:2013). Es esencial que una organización identifique sus requisitos de seguridad. Existen tres fuentes principales para los requisitos de seguridad:

a) La evaluación de los riesgos de la organización, teniendo en cuenta los objetivos y estrategia de negocio globales de la organización. A través de una evaluación de los riesgos se identifican las amenazas de los activos, se evalúa la vulnerabilidad y la probabilidad de su ocurrencia y se estima su impacto potencial;
b) El conjunto de requisitos legales, estatutarios, regulatorios y contractuales que debería satisfacer la organización, sus socios comerciales, contratistas y proveedores de servicios, así como su entorno socio-cultural;

c) El conjunto de principios, objetivos y requisitos de negocio que la organización ha desarrollado para el manejo, tratamiento, almacenamiento, comunicación y archivo de la información que da soporte a sus operaciones.

Para la aplicación de los controles es necesario tener en cuenta la evaluación de riesgos, conjunto de requisitos legales que debe compensar la organización y principios, objetivos desarrollados y aplicados por la misma organización; con la evaluación de riesgos se deberá llevar a cabo la matriz de los activos y la identificación de vulnerabilidades, su ocurrencia y el impacto sobre los activos.

Selección de controles

De acuerdo a la (ISO/IEC 27002:2013) Los controles pueden elegirse de los controles de esta norma o de otros conjuntos de controles, o bien se pueden diseñar nuevos controles para cubrir adecuadamente las necesidades específicas.

También la (ISO/IEC 27002:2013) establece que, la selección de los controles depende de las decisiones de carácter organizativo basadas en los criterios de aceptación del riesgo, las opciones de tratamiento del riesgo y de los enfoques generales de gestión del riesgo aplicados en la organización, y debería depender también de toda la legislación y reglamentación nacional e internacional aplicable. La selección de los controles también depende del modo en que los controles interactúan para proporcionar una protección en profundidad.

Varios de los controles de norma ISO/IEC 27002, se pueden considerar como principios que guiaran la gestión de la seguridad de la información y sus activos, los cuales son aplicables en la mayoría de las organizaciones.

Desarrollo de directrices propias

La (ISO/IEC 27002:2013) plantea que, esta norma internacional puede verse como un punto de partida para desarrollar unas directrices específicas para la

organización. Pueden no ser aplicables todas las recomendaciones y controles de este código de prácticas. Incluso, pueden requerirse controles adicionales que esta norma no incluye. Cuando esto suceda puede ser útil mantener referencias cruzadas de los capítulos de esta norma con otros documentos que contengan directrices adicionales de controles, que faciliten la comprobación del cumplimiento a los auditores y a otros socios de la organización.

Se debe tener en cuenta que la norma ISO/IEC 27002 permite la creación de nuevas directrices a partir del uso de guías y referencias cruzadas que complementan los controles o adicionan controles propios para la organización que faciliten su cumplimiento.

Consideraciones del ciclo de vida

La (ISO/IEC 27002:2013) establece que, la información tiene un ciclo de vida natural, desde la creación y el origen de la misma pasando por el almacenamiento, tratamiento, utilización y transmisión hasta su eventual destrucción o deterioro. El valor y los riesgos para los activos puede variar durante su tiempo de vida (por ejemplo, la difusión no autorizada o el robo de las cuentas financieras de una empresa es mucho menos importante después de que hayan sido publicados oficialmente), pero la seguridad de la información continúa siendo importante en todas las etapas.

Al igual la (ISO/IEC 27002:2013) dice, los sistemas de información tienen ciclos de vida en los cuales son concebidos, especificados, diseñados, desarrollados, probados, implantados, utilizados, mantenidos y, finalmente, retirados del servicio y eliminados. La seguridad de la información debería ser tenida en cuenta en todas estas etapas. Los nuevos desarrollos del sistema y los cambios en los sistemas actuales presentan oportunidades para que las organizaciones actualicen y mejoren los controles de seguridad, teniendo en cuenta tanto los incidentes reales como los riesgos de seguridad asociados a incidentes actuales y futuros.

Para la consideración del ciclo de vida de la información y activos, es propia de la organización, pero deberá estar sujeta a controles, cambios y actualizaciones, porque en el paso del tiempo se van encontrando nuevos riesgos al igual que soluciones definitivas sobre los activos e información.

Objeto y campo de aplicación

Para la (ISO/IEC 27002:2013) Esta norma internacional establece directrices para la seguridad de la información en las organizaciones y prácticas de gestión de la seguridad de la información incluyendo la selección, la implantación, y la gestión de los controles teniendo en consideración el entorno de riesgos de seguridad de la información de la organización.

Esta norma internacional está diseñada para ser utilizada en organizaciones que pretendan:

a) seleccionar controles en el proceso de implantación de un Sistema de Gestión de la Seguridad de la Información basado en la Norma ISO 27001 (ISOTools Excellence, s. f.);
b) implantar controles de seguridad de la información comúnmente aceptados;
c) desarrollar sus propias directrices de seguridad de la información.

El principal objetivo de la Norma ISO/IEC 27002 no es solo implantar y seleccionar controles, también ayuda al desarrollo de propias directrices para la organización, está sujeta a cambios, los controles pueden ser parciales dependiendo del proceso al que se le aplique.

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Caracterización de la organización

Misión

Somos una empresa dedicada al ensamblaje de partes y vehículos automotores de calidad.

Fomentamos el desarrollo de la Provincia y el País, así como también el crecimiento de nuestra gente generando al mismo tiempo la rentabilidad necesaria para asegurar la continuidad y desarrollo de nuestra organización.

Visión

Nuestra cultura organizacional impulsa la búsqueda de la excelencia en un ambiente acogedor que facilita el desarrollo de nuestro equipo humano.

Mantenemos procesos de fabricación innovadores, confiables, seguros y competitivos que nos permiten ensamblar vehículos de calidad.

Fomentamos el desarrollo de la industria a través del crecimiento paulatino del número de unidades que ensamblamos y del tipo de partes locales que instalamos en nuestros vehículos, lo que nos permite adoptar y transferir tecnología, generando nuevos y mejores negocios para todas las partes involucradas con nuestra organización.

Gestionamos nuestros procesos de acuerdo a los requisitos establecidos en la norma ISO 9001, lo que nos brinda las herramientas y los recursos necesarios para trabajar ordenadamente y con calidad, facilitándonos el logro de la satisfacción de nuestros clientes internos y externos.

Logramos clientes entusiasmados con nuestros productos, esto nos permite construir un gran nombre de respaldo y seriedad asegurando el crecimiento y sustentabilidad de nuestro negocio.

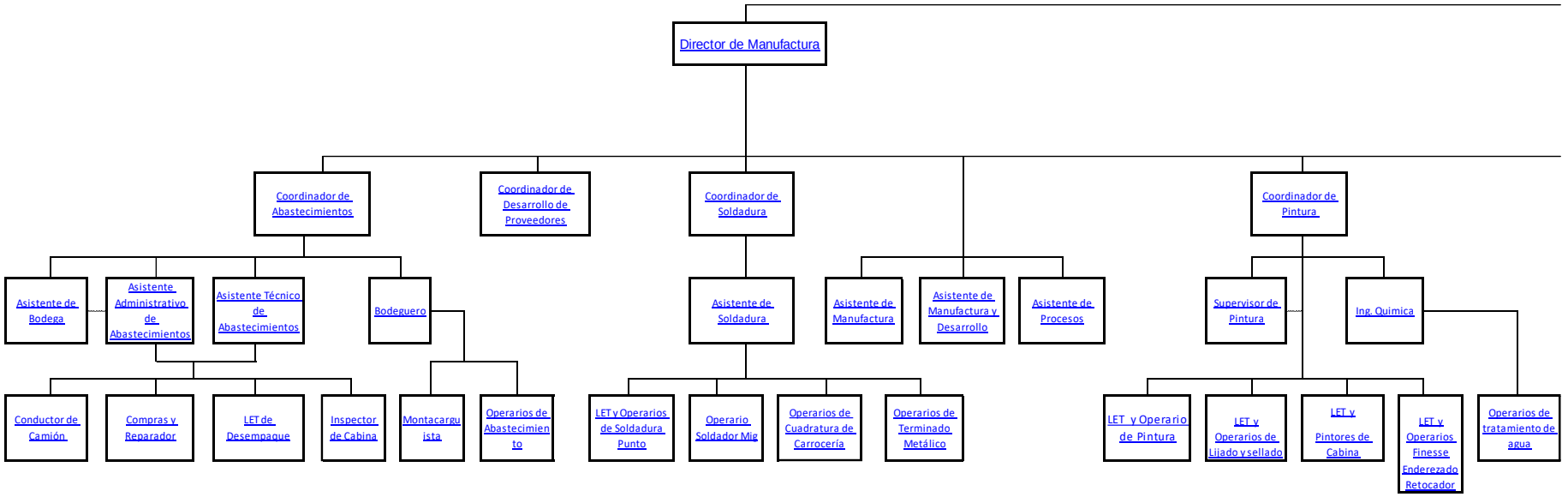
Generamos la rentabilidad adecuada para asegurar la continuidad y desarrollo de nuestra empresa, así como de la sociedad.

Política de calidad

Somos una empresa dedicada al ensamblaje de partes y vehículos automotores de calidad. Estamos comprometidos con el cumplimiento de los requisitos de la norma ISO 9001 que nos permite mantener la integridad y eficacia de nuestro Sistema de Gestión, así como su Mejora Continua.

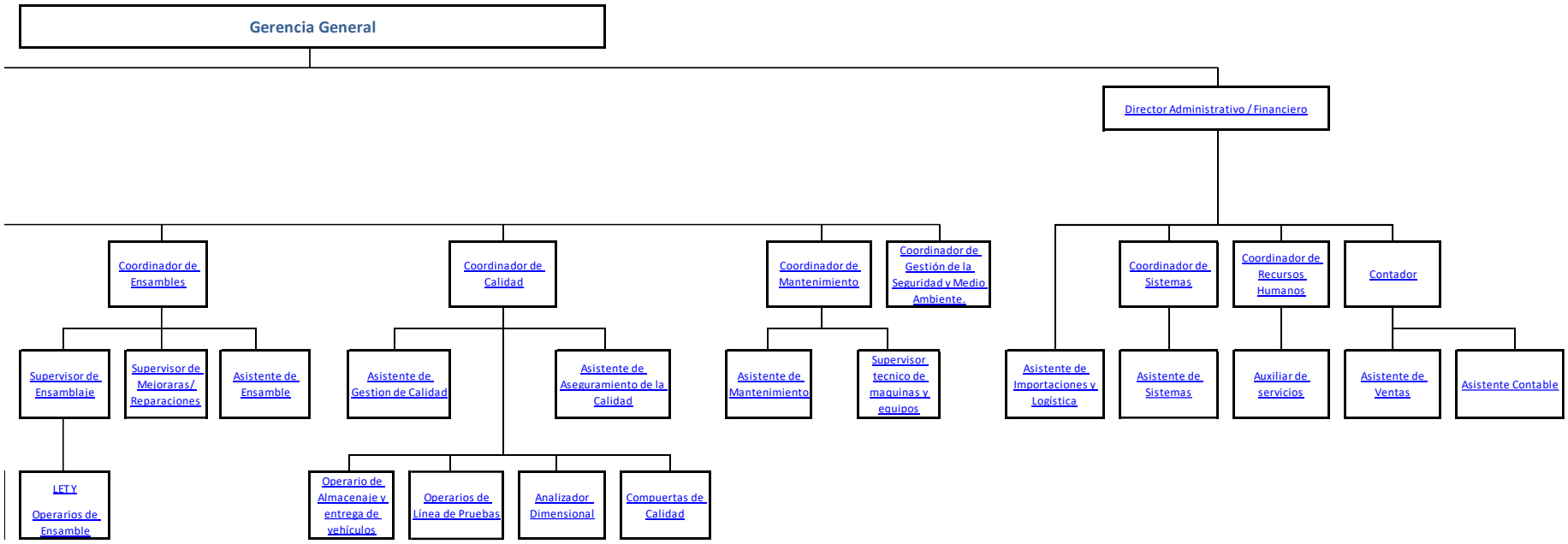
Organigrama

Gráfico 3. Organigrama holding de empresas parte 1



Fuente: SGC - ISO 9001 MC-01 Anexo A - Estructura Funcional V8 implementado en la empresa

Gráfico 4. Organigrama holding de empresas parte 2



Fuente: SGC - ISO 9001 MC-01 Anexo A - Estructura Funcional V8 implementado en la empresa

Como trabaja el proceso de TI

Asesorar a la organización en la búsqueda de las alternativas más adecuadas en materia de Recursos Informáticos (*hardware y software*) así como en el establecimiento de los mejores recursos en comunicaciones.

Implementar soluciones de *hardware, software* y recursos de comunicación, así como realizar el seguimiento del funcionamiento de las mismas.

Mantener en condiciones óptimas los recursos informáticos y de comunicaciones de la organización aplicando las seguridades pertinentes y velando por su disponibilidad.

Brindar soporte técnico en las actividades de los usuarios cuando se lo requiera.
Proveer de la capacitación necesaria y requerida para el uso correcto y eficiente de los recursos informáticos de la organización.

Administrar los sistemas ERP de la organización, así como respaldar y gestionar las bases de datos correspondientes.

Mejorar los procesos de la organización soportados en los Recursos Informáticos.

Velar por el correcto desempeño del Proceso de Gestión de Sistemas, así como realizar reportes e informes correspondientes a los resultados de la gestión del mismo.

Colaborar con todas las actividades que la organización lo demande para el logro de sus objetivos.

Proveer eficaz y eficientemente de asistencia en procesos informáticos, necesarios para soportar y vincular el correcto desempeño de las actividades del personal.

Mantener en condiciones óptimas los recursos informáticos y de comunicaciones de la organización aplicando las seguridades pertinentes y velando por su disponibilidad.

Realizar los mantenimientos necesarios en hardware y software que permitan la continuidad de servicios informáticos.

Administrar los servidores de antivirus, para una correcta actualización y supervisión de usuarios.

Realizar reportes e informes correspondientes a los resultados de la gestión del mismo.

Beneficios del proyecto dentro de la organización

Los beneficios se centran en gestionar los diferentes controles de seguridad con el objetivo de proteger los activos de la organización resolviendo, manejando y mitigando las diferentes vulnerabilidades, a través de herramientas de protección y estableciendo estándares de seguridad que en su desarrollo proporcionan:

Privacidad: los servicios de seguridad permiten conservar de forma efectiva los datos privados de empleados y clientes. El no mantener protegidos los datos puede darse a la perdida, fuga o mal uso de la información.

Protección: permitirá proteger los equipos dotando de seguridad al software y al hardware, lo cual mantendrá su entereza y prolongará el buen funcionamiento.

Integridad: el proteger el almacenamiento de datos de los diferentes equipos y dispositivos con aplicaciones de seguridad colaboran en proteger de forma integral los datos y los equipos. De ese modo puede evitarse la manipulación de información y garantizara que la información sea verdadera y precisa.

Prevención: el mantener un sistema de seguridad informática, permite prevenir i evitar riesgos, es decir, anticipara las intrusiones obstaculizando el peligro.

Autenticación: se permite el acceso a la información a los usuarios autorizados mediante códigos de verificación y otros métodos de autenticación.

Productividad: Garantizará el trabajo continuo, evitando detenciones.

Control: será posible realizar comprobaciones internas, monitorizando el estado de los equipos y dispositivos mediante la inspección de amenazas.

Accesibilidad: Es de gran importancia mantener los protocolos de seguridad. La accesibilidad hace posible que los usuarios autorizados tengan acceso constante a los datos haciendo uso de la información siempre que lo necesiten y minimizando los riesgos.

Con los beneficios antes mencionados podemos concluir que lo más importante es garantizar la seguridad de los activos y gestión de datos en información, ante una actualización constante de la tecnología de la información. Por lo tanto, es necesario reforzar la seguridad informática y tomar las medidas adecuadas para mitigar los diferentes riesgos.

2.2. Metodología de investigación

Investigación cuantitativa

Según (Hernández-Sampieri, 2018) y (Villalobos Zamora, 2019) la investigación cuantitativa pretende establecer el grado de asociación o correlación entre variables, la generalización y objetivación de los resultados por medio de una muestra permite realizar inferencias causales a una población que explican por qué sucede o no determinado hecho o fenómeno.

Para (Guadalupe & Concepción, 2020) “consiste en contrastar hipótesis desde el punto de vista probabilístico y, en caso de ser aceptadas y demostradas en circunstancias distintas, a partir de ellas elaborar teorías generales”.

(Hernández-Sampieri, 2018) señala que en las investigaciones cuantitativas predomina la cantidad y su manejo estadístico matemático y los informantes tienen un valor igual.

La investigación cuantitativa está orientada a comprobar y verificar de manera deductiva las proposiciones planteadas durante la investigación, para esto se plantea hipótesis en función de la relación de variables que serán sometidas a medición y así lograr la confirmación o refutación.

No experimental

(Behar et al., 2021) señala que en ellas el investigador observa los fenómenos tal y como ocurren naturalmente, sin intervenir en su desarrollo.

Para (Hernández-Sampieri, 2018) es aquella que se realiza sin manipular deliberadamente variables. Se basa fundamentalmente en la observación de fenómenos tal y como se dan en su contexto natural para analizarlos con posterioridad. En este tipo de investigación no hay condiciones ni estímulos a los cuales se expongan los sujetos del estudio. Los sujetos son observados en su ambiente natural.

Las investigaciones no experimentales, la variable independiente ya ha ocurrido cuando el investigador realizara el estudio. Es por esta característica, los estudios que se trabajan bajo estas circunstancias son investigaciones ex post facto.

Diseño transeccional

Para (Rodríguez et al., 2021) Los diseños de investigación transeccional o transversal recolectan datos en un solo momento, en un tiempo único. Su propósito es

describir variables, y analizar su incidencia e interrelación en un momento dado. Es como tomar una fotografía de algo que sucede. Por ejemplo, investigar el número de empleados, desempleados y subempleados en una ciudad en cierto momento. O bien, determinar el nivel de escolaridad de los trabajadores de un sindicato, en un punto en el tiempo. O tal vez, analizar la relación entre la autoestima y el temor de logro en un grupo de atletas de pista (en determinado momento). O bien, analizar si hay diferencias en contenido de sexo entre tres telenovelas que están exhibiéndose simultáneamente.

Según (Hernández-Sampieri, 2018) Se utiliza cuando la investigación se centra en analizar cuál es el nivel o estado de una o diversas variables en un momento dado o bien en cual es la relación entre un conjunto de variables en un punto en el tiempo. En este tipo de diseño se recolectan datos en un solo momento, en un tiempo único. Su propósito esencial es describir variables y analizar su incidencia e interrelación en un momento dado. Pueden abarcar varios grupos o subgrupos de personas, objetos o indicadores

Cuando la investigación se centra en analizar cuál es el nivel o estado de una o diversas variables en un momento dado o bien en cuál es la relación entre un conjunto de variables en un punto en el tiempo, se utiliza el diseño transeccional.

En este tipo de diseño se recolectan datos en un solo momento, en un tiempo único o momento dado.

Instrumentos

Diseños o estructuras

Para la valoración de datos y activos se usó una combinación de una escala cualitativa, donde los criterios van desde un nivel leve a un nivel muy severo, una escala alta para la organización. Esta propuesta se basa en la desarrollada por (Velepucha Sánchez et al., 2022), que establecieron un criterio de leve a muy severo, siendo leve “despreciable” y muy severo “extremo”. En la siguiente tabla

se puede observar con mayor claridad los criterios de valoración de datos y activos que serán usados.

Tabla 2. Grados de negatividad.

Grado de negatividad	Confidencialidad	Integridad	Disponibilidad
Leve	¿Qué importancia tendría que el activo o dato fuera conocido por personas no autorizadas?	¿Qué importancia tendría que los datos o activos fueran removidos o modificados sin supervisión?	¿Qué importancia tendría que los datos o activos no estén disponibles?
Moderada			
Severa			
Muy severa			

Fuente Adaptación propia del texto de Amutio & González (2012)

Metodología para valoración de riesgos

El producto entre probabilidad e impacto determinará el nivel de riesgo del evento de contingencia que se valore y que afecte al activo de tecnología de información (Santos-Olmo et al., 2020).

A continuación, se describen los valores para la probabilidad, y para el impacto definidos en la metodología de riesgo operacional elaborado por (Santos-Olmo et al., 2020):

Tabla 3. Frecuencia de evento

Probabilidad	Descripción
Poco frecuente	Este grado de probabilidad indica que un evento tiene una baja posibilidad de ocurrir. Es raro y sucede en contadas ocasiones, con baja incidencia histórica o predictiva.
Aleatorio	Este grado de probabilidad sugiere que un evento ocurre de manera irregular y sin un patrón claro. La ocurrencia es impredecible y no se puede anticipar con precisión.
Muy frecuente	Este grado de probabilidad señala que un evento tiene una alta posibilidad de ocurrir. Sucede regularmente y es común en la mayoría de las circunstancias, con alta incidencia histórica o predictiva.

Fuente Adaptación propia del texto de Klever Pilamunga y Isaac Maliza 2018

Tabla 4. Grados de impacto: bajo, medio, alto.

Impacto	Descripción
Bajo	El impacto es mínimo y no causa daños significativos. Las operaciones normales pueden continuar con poca o ninguna interrupción, y los costos asociados a la recuperación son bajos.
Medio	El impacto es moderado, causando interrupciones notables en las operaciones y requiriendo esfuerzos considerables para la recuperación. Puede haber daños financieros y operativos manejables, pero significativos.
Alto	El impacto es severo y puede resultar en interrupciones críticas de las operaciones, con daños financieros y operativos significativos. La recuperación requiere tiempo y recursos considerables, afectando seriamente a la organización.

Fuente Adaptación propia del texto de Klever Pilamunga y Isaac Maliza 2018

Evaluación de controles ISO/IEC 27002

Por parte de *Information security* (2017) se desarrolló una herramienta/instrumento, la cual se usó para medir la madurez del desarrollo de la política de seguridad y será aplicada en una consulta o validación de expertos.

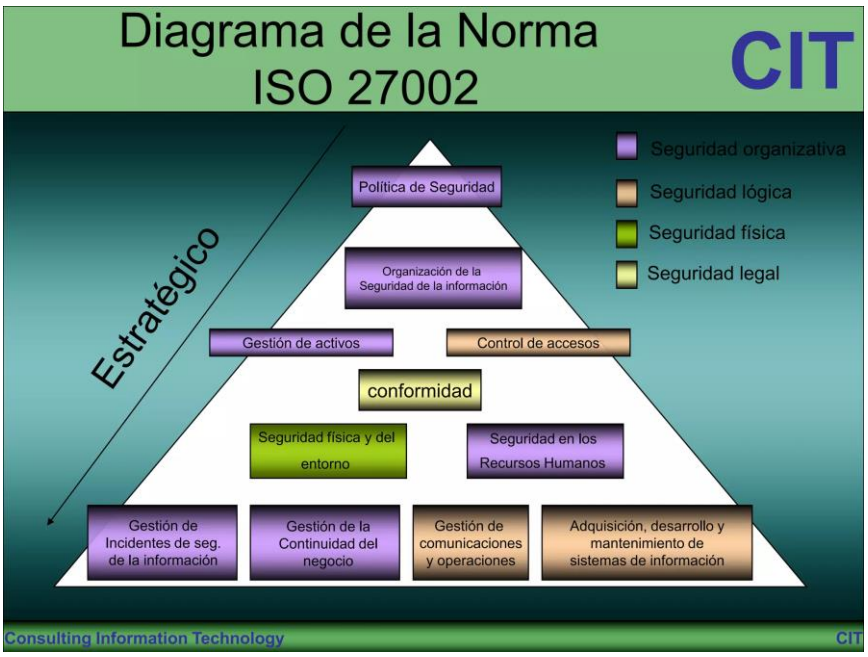
2.3. Metodología de desarrollo

Funcionamiento de la metodología

El fin de realizar el análisis de las operaciones críticas, sirvió para determinar las tareas, procesos y servicios, aquellos activos que se encuentran dentro de la infraestructura del proceso de tecnologías de la información.

Con la definición de operaciones y activos críticos, se procedió a evaluar mediante una matriz de riesgos, donde se identificó diferentes amenazas y vulnerabilidades las cuales fueron evaluadas conforme a su impacto potencial y la probabilidad de que ocurran.

Gráfico 5. Diagrama de la norma ISO 27002



Fuente: Consulting Information Technology (2013)

Requisitos

Minimización de riesgos

En base al plan de contingencia desarrollado para satisfacer las necesidades de control en el SGC de la empresa en base a la norma ISO 9001 / 2015 se desarrollaron las siguientes tablas para la matriz de riesgos.

Grados de negatividad: leve, moderada, severa, muy severa.
Frecuencias de evento: poco frecuente, aleatorio, muy frecuente
Grados de impacto: bajo, medio, alto.

En caso de ocurrir incidentes a lo que correspondería incendio o acción del fuego se creó la siguiente tabla para mitigar los diferentes riesgos, donde se expresa la situación actual o implementación y la acción correctiva el cumplimiento de la misma.

Tabla N 5: Parámetros de contingencia en caso de incendio o fuego.

Incendio o Fuego	
Grado de Negatividad: Muy Severo	
Frecuencia de Evento: Aleatorio	
Grado de Impacto: Alto	
Situación Actual	**Acción Correctiva**
La oficina donde están ubicados los servidores cuenta con un extintor cargado, ubicado muy cerca a esta oficina. De igual forma cada piso cuenta con un extintor debidamente cargado.	Se cumple
No se ha ejecutado un programa de capacitación sobre el uso de elementos de seguridad y primeros auxilios, a los funcionarios nuevos, lo que no es eficaz para enfrentar un incendio y sus efectos	Se realizó capacitación para el manejo de extintores y primeros auxilios.
El servidor realiza backups de la información diariamente, pero no existe ninguna otra copia de respaldo.	Realizar backups del servidor de forma mensual, almacenada en DVD, ubicarlos, guardarlos de manera segura y donde no sufran daños.

Fuente: SGC - ISO 9001 SOP-07-PL- 04 - PLAN DE CONTINGECIA EQUIPOS CRITICOS

Para la mitigación de fallas que pueden presentarse en los equipos a las situaciones actuales como fallas por mantenimiento, hardware o energía eléctrica se plantearon, acciones correctivas que ayudan para solventar cada uno de los casos en la siguiente tabla.

Tabla N 6: Parámetros de contingencia en caso de fallas en los equipos.

Falla en los Equipos	
Grado de Negatividad: Grave	
Frecuencia de Evento: Aleatorio	
Grado de Impacto: Grave	
Situación Actual	**Acción Correctiva**
La falla en los equipos muchas veces se debe a falta de mantenimiento y limpieza.	Realizar mantenimiento preventivo de equipos por lo menos dos veces al año.
La falla en el hardware de los equipos requiere de remplazo de repuestos de forma inmediata.	Contar con proveedores en caso de requerir remplazo de piezas y de ser posible contar con repuestos de quipos que están para dar de baja.
El daño de equipos por fallas en la energía eléctrica, requiere contar con dispositivos que amplíen tiempo para apagar correctamente el equipo.	Se cumple. La CMV en su mayoría cuenta con portátiles por tanto se recomienda que cada funcionario mantenga cargado su equipo y los de escritorio cuenta con UPS.

Fuente: SGC - ISO 9001 SOP-07-PL- 04 - PLAN DE CONTINGECIA EQUIPOS CRITICOS

En caso de infección o ataques por virus informáticos se presenta los siguientes casos para solventar y/o mitigar, con ciertos parámetros y adecuaciones que se deben revisar periódicamente.

Tabla N 7: Parámetros de contingencia en caso de infección por virus informáticos.

Acción de Virus Informático	
Grado de Negatividad: Muy Severo	
Frecuencia de Evento: Continuo	
Grado de Impacto: Grave	
Situación Actual	**Acción Correctiva**
Se cuenta con un software antivirus para la entidad, pero su actualización no se realiza de forma inmediata a su expiración.	Se debe evitar que las licencias de antivirus expiren, se requiere renovación con anterioridad del nuevo antivirus.
Únicamente el área de sistemas es la encargada de realizar la instalación de software en cada uno de los equipos de acuerdo a su necesidad.	Se cumple
Se tiene acceso restringido al servidor, únicamente es el administrador de la red el encargado de cambiar configuraciones y anexar nuevos equipos.	Antes de ingresar una maquina a la red, se debe comprobar la existencia de virus en la misma.
Los antivirus no se actualizan periódicamente en cada equipo.	Informar la política informática de actualización de antivirus a cada funcionario y su responsabilidad frente a esto.

Fuente: SGC - ISO 9001 SOP-07-PL- 04 - PLAN DE CONTINGECIA EQUIPOS CRITICOS

Para mitigar los diferentes casos de accesos no autorizados, sean estos a redes de internet, accesos a usuarios, o compartición de información de acceso se plantea en la tabla a continuación las siguientes resoluciones.

Tabla N 8: Parámetros de contingencia para accesos no autorizados.

Accesos No Autorizados	
Grado de Negatividad: Grave	
Frecuencia de Evento: Aleatorio	
Grado de Impacto: Grave	
Situación Actual	**Acción Correctiva**
Se controla el acceso al sistema de red mediante la definición de un administrador con su respectiva clave.	Se cumple
La asignación de usuario se realiza a discrecionalidad del técnico de sistemas y se solicita de forma verbal.	Se debe solicitar por escrito (E-mail) al técnico de sistemas la creación de usuarios y los permisos que se requiere sean asignados, o cualquier cambio referente a los mismos.
La oficina administrativa no comunica al área de sistemas, cuando un funcionario sale a vacaciones o se retira de la entidad a fin de desactivar ese usuario.	Se debe informar al área de sistemas, que funcionario sale a vacaciones para así bloquear el respectivo usuario por el tiempo de ausencia, igualmente en caso de retiro definitivo.
Se acostumbra a confiar la clave de acceso (uso personal) a compañeros de área, sin medir la implicación en el caso de acceso no autorizado.	Capacitar al personal sobre la confidencialidad de sus contraseñas, recalcando la responsabilidad e importancia que ello implica, sobre todo para el manejo de software.

Fuente: SGC - ISO 9001 SOP-07-PL- 04 - PLAN DE CONTINGECIA EQUIPOS CRITICOS

En la tabla siguiente se detallan diferentes tipos de riesgos y eventos que ocasionan, los mismos afectan a la organización y los usuarios de diferentes formas a los cuales se les dio una ponderación del grado de impactó y la frecuencia con la que ocurre cada evento.

Tabla N 9: Parámetros de contingencia para otros eventos

EVENTOS CONSIDERADOS EN EL PLAN DE CONTINGENCIA			
RIESGO	**EVENTO**	**GRADO DE IMPACTO**	**FRECUENCIA DEL EVENTO**
·Fallas Corte de Cable UTP. ·Fallas Tarjeta de Red. ·Fallas IP asignado. ·Fallas Punto de Swicht. ·Fallas Punto Pacht Panel. ·Fallas Punto de Red.	NO EXISTE COMUNICACIÓN ENTRE CLIENTE Y SERVIDOR	MEDIO	MUY FRECUENTE
Corte General del Fluido eléctrico	INTERRUPCIÓN DEL FLUIDO ELÉCTRICO DURANTE LA EJECUCIÓN DE LOS PROCESOS.	SEVERO	POCO FRECUENTE
·Fallas de Componentes de Hardware del Servidor. ·Falla del UPS (Falta de Suministro eléctrico). ·Virus. ·Sobrepasar el límite de almacenamiento del Disco ·Computador de Escritorio funciona como Servidor	FALLAS EN EL EQUIPO SERVIDOR	MUY SEVERO	POCO FRECUENTE
·Falla de equipos de comunicación: SWITCH, Antenas, ·Fibra Óptica. ·Fallas en el software de Acceso a Internet. ·Perdida de comunicación con proveedores de Internet.	PERDIDA DE SERVICIO DE INTERNET	MEDIO	POCO FRECUENTE

Fuente: SGC - ISO 9001 SOP-07-PL- 04 - PLAN DE CONTINGECIA EQUIPOS CRITICOS

Selección de numerales y categorías de control.

La selección de numerales y categorías de control se lo realiza conforme al uso y aplicación para el *Holding* de empresas, en base a las tablas expuestas en el punto anterior y también que servirán de mejora o complementación para lo existente en el SGC de cada empresa.

- Política de seguridad de la información
  - Política para la seguridad de la información
  - Revisión de la política de seguridad de la información
- Dispositivos móviles y teletrabajo
  - Política de dispositivos móviles
  - Teletrabajo
- Durante el empleo
  - Sensibilización, educación y formación en materia de seguridad de la información
  - Cese o cambio de responsabilidades laborales
- Responsabilidad de los activos
  - Inventario de activos y otros activos asociados
  - Uso aceptable de los activos
  - Devolución de activos
- Clasificación de la información
  - Clasificación de la información
  - Etiquetado de la información
  - Uso aceptable de la información y otros activos asociados.
- Manejo de los medios de almacenamiento
  - Medios de almacenamiento
- Requisitos empresariales del control de acceso
  - Control de acceso
- Gestión del acceso de los usuarios
  - Registro y baja de usuarios
  - Derechos de acceso
  - Derecho de accesos privilegiado
  - Información de autenticación
- Control de acceso al sistema y a las aplicaciones
  - Restricción de acceso a la información
  - Autenticación segura
  - Sistema de gestión de contraseñas
  - Uso de programas de utilidad privilegiados
  - Acceso al código fuente

- Controles criptográficos
  - Uso de la criptografía
- Zonas seguras
  - Parámetros de seguridad física
  - Entrada física
  - Asegurar las oficinas, salas e instalaciones
  - Protección contra las amenazas físicas y medioambientales
- Seguridad en los equipos
  - Ubicación y protección de los equipos
  - Seguridad del cableado
  - Mantenimiento de los equipos
  - Seguridad de los activos fuera de las instalaciones
  - Eliminación segura y reutilización de equipos
  - Dispositivos de punto final del usuario
  - Escritorio y pantalla despejados
- Protección contra el malware
  - Controles contra el malware
- Copia de seguridad
  - Información de respaldo
  - Realización y frecuencia del respaldo
- Registro y control
  - Registro
  - Registro de administración y operación
  - Sincronización de relojes
- Control de software operativo
  - Instalación de software es sistemas operativos
  - Gestión de vulnerabilidades técnicas
  - Restricción en la instalación del software.
- Consideración sobre la auditoria de los sistemas de información
  - Protección de los sistemas de información durante la auditoria
- Gestión de la seguridad de red
  - Seguridad en las redes
  - Seguridad en los servicios de red

- Segregación de redes
- Intercambios de información
  - Transferencia de información
  - Acuerdos de confidencialidad y no divulgación
- Seguridad en los procesos de desarrollo y apoyo
  - Ciclo de vida de desarrollo seguro
  - Gestión del cambio
  - Arquitectura de sistemas seguros y principios de ingeniería
  - Separación de entornos de desarrollo, pruebas y producción
  - Desarrollo externalizado
  - Pruebas de seguridad en el desarrollo y la aceptación
- Gestión de incidentes y continuidad de la seguridad de la información
  - Planificación y preparación de la gestión de incidentes de seguridad
  - Informe de eventos de seguridad de la información
  - Evaluación y decisión sobre los eventos
  - Respuesta a los incidentes de seguridad de la información
  - Aprender de los incidentes de seguridad de la información
  - Recogida de pruebas
  - Seguridad de la información durante la interrupción
  - Preparación de las TIC para la continuidad de la actividad
- Cumplimiento de los requisitos legales y contractuales
  - Requisitos legales, reglamentarios y contractuales
  - Derechos de propiedad intelectual
  - Privacidad y protección de la información personal
- Revisiones de la seguridad de la información
  - Revisión independiente de la seguridad de la información
  - Cumplimiento de las políticas y normas de seguridad
  - Revisión de la conformidad técnica.

Desarrollo de la propuesta

POLÍTICA DE SEGURIDAD INFORMÁTICA

Introducción

La entidad Ciudad del Auto CIAUTO Cía. Ltda. tiene en cuenta la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la organización, razón por la cual es necesario que se establezca un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

Este documento describe las directivas y normas de seguridad de la información definidas por las entidades del sector asegurador. Para la elaboración del mismo, se toman como base las regulaciones aplicables y las recomendaciones del estándar ISO 27002.

Las políticas incluidas en este manual se constituyen como parte fundamental del sistema de gestión de seguridad de la información de la entidad y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos. La seguridad de la información es una prioridad para la entidad y por tanto es responsabilidad de todos velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.

Objetivos

- Formalizar el procedimiento de Gestión de Seguridad de la Información, que hace parte del proceso de Gestión de Riesgos y Control.
- Definir y reglamentar los procedimientos requeridos para la operación del Sistema de Gestión de Tecnologías de la Información, con el fin de asegurar que se ejecuten las actividades requeridas para proteger la información de las amenazas que recaigan sobre ella.

- Generar una cultura para disminuir el riesgo de información que le permita a la Entidad mantener el monitoreo, control y medición de las amenazas y vulnerabilidades, y aplicar procedimientos que salvaguarden la confidencialidad, integridad, disponibilidad y privacidad de la información.

Alcance

Esta propuesta reglamenta el proceso, desde la definición de políticas y la planeación, hasta el mejoramiento del proceso, pasando por la implementación de los planes, la ejecución y monitoreo continuo, esquematizando lecciones, aplicando nuevas y mejores prácticas.

Glosario

- **Activo de Información:** Es un dato o elemento que tiene valor para la Entidad.
- **Amenaza:** Hecho que puede producir un daño provocado por un evento.
- **ASI:** Analista de Seguridad de la Información.
- **Auditoria.** Practica de buen gobierno que permite identificar el nivel de cumplimiento y adherencia dentro de la organización a las normas, principios o buenas prácticas de la disciplina que se está analizando.
- **Confidencialidad:** Seguridad de que la información es accesible solamente por quienes están autorizados para ello.
- **Disponibilidad:** Seguridad de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando los requieren.
- **Dispositivo de almacenamiento de información**: Cualquier elemento fijo o removible que haga parte de un equipo o que pueda ser conectado a los equipos de procesamiento o transmisión de información, en el que resida o pueda residir información, entre los más conocidos están: memorias USB, dispositivos de reproducción de multimedia, unidades de CD-DVD fijas o removibles, Tape Back-ups, unidades de disco USB, unidades de ZIP Driver, cámaras fotográficas, dispositivos móviles.

- **Doble Participación.** Principio por el cual un empleado no puede concentrar varias funciones dentro de un mismo proceso para llevar a cabo, de forma unilateral, labores de modificación y/o aprobaciones.
- **Dueño de la Información:** Un individuo o unidad organizacional que tiene responsabilidad por clasificar y tomar decisiones de control con respecto al uso de su información.
- **Evento:** Suceso repentino que puede generar alguna afectación o alarma en un sistema de información.
- **Incidente:** Hecho o evento que puede afectar un activo de información.
- **Integridad:** Protección de la exactitud, del estado completo de la información y de los métodos de procesamiento.
- **Logs:** Registro oficial de eventos durante un periodo de tiempo en particular. Identifica información sobre quién, qué, cuándo, dónde y por qué un evento ocurre en cualquier sistema de información.
- **Norma:** Conjunto de reglas requeridas para implantar las políticas. Las normas hacen mención específica de tecnologías, metodologías, procedimientos de aplicación y otros factores involucrados y son de obligatorio cumplimiento.
- **Nivel de Sensibilidad:** Es un indicador del valor o importancia que tiene la información para la organización, dependiendo de la clasificación asignada a cada uno de las características de integridad, disponibilidad y privacidad de dicha información.
- **Procedimientos:** Pasos operacionales específicos que los individuos deben tomar para lograr las metas definidas en las políticas.
- **Riesgo:** Probabilidad de ocurrencia de un evento de seguridad.
- **Seguridad física:** La protección de los equipos de procesamiento de la información de daños físicos, destrucción o robo; Protege las facilidades asignadas para el procesamiento de la información de daño, destrucción o ingreso desautorizados; y al personal de las situaciones potencialmente dañosas.
- **Seguridad de la Información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar

otras propiedades tales como: autenticidad, trazabilidad, no repudio y afinidad.

- **Segregación de Funciones.** Principio por el cual se reglamentan las funciones de uno o más funcionarios para la implementación del principio de la doble participación. Igualmente, dichas funciones no deben ser contradictorias entre sí o sobreponer responsabilidades entre los actores de un procedimiento.
- **Sistema de Gestión de las tecnologías de la Información:** Parte del sistema de gestión global basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es garantizar que los riesgos de la seguridad de la información son conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.
- El Sistema de Gestión incluye la estructura organizacional, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos, recursos.
- **Usuarios:** Un individuo que tiene autoridad limitada y específica del dueño de información para ver, modificar, adicionar, divulgar o eliminar información.
- **Vulnerabilidad:** Debilidad de un sistema que compromete la integridad, disponibilidad o la confidencialidad del mismo.
- **VPN:** Tecnología de red, que permite una extensión segura de la red local sobre una red pública o no controlada.

Políticas, procedimientos y controles

- **Política de la seguridad de la información**

  Directrices establecidas para la seguridad de la información

  Objetivo: Brindar orientación y apoyo, para la seguridad de la información de acuerdo con los requisitos de negocio, las leyes y reglamentos pertinentes.

  - ✓ **Política para la seguridad de la información**

    Control

    Definir un conjunto de políticas para la seguridad de la información, aprobada, publicada y comunicada a los empleados en todos los procesos.

    Guía de implementación

    La política de seguridad de la información deberá abordar los requisitos creados por:

    - Estrategia de negocio
    - Reglamentaciones, legislaciones y contratos
    - En el entorno actual tener una proyección de amenazas a la seguridad de la información.

    La política de la seguridad de la información deberá tener declaraciones concernientes a:

    - Definir objetivos y principios para orientar todas las actividades relacionadas a la seguridad de la información.
    - Asignación de responsabilidades generales y especificas a cada rol para la gestión de la información.
    - Procesos para el manejo de desviaciones y excepciones.

    Información adicional

    Si alguna de las políticas de seguridad de la información se distribuye por fuera de la organización, se deberá tener cuidado de no revelar información confidencial.

- ✓ **Revisión de la política de seguridad de la información**

  Control

  La política para la seguridad de la información deberá ser revisada en intervalos planificados, o en el caso de ocurrir cambios significativos, para asegurar la adecuación y eficacia continua.

  Guía de implementación

  La política de seguridad deberá tener un propietario que tenga la responsabilidad, para el desarrollo, revisión y evaluación de las políticas. La revisión deberá incluir la valoración de las oportunidades de mejora y el enfoque para la gestión de los cambios en respuesta a la seguridad de la información.

- ➢ **Política de la seguridad de la información**

  Objetivo: garantizar la seguridad en el proceso de teletrabajo y el buen uso de dispositivos móviles.

  - ✓ **Política de dispositivos móviles**

    Control

    Adoptar políticas y medidas de seguridad de soporte, para la gestión de los riesgos introducidos por el uso de dispositivos móviles.

    Guía de implementación

    La política de dispositivos móviles deberá considerar:

    - Registro de los dispositivos móviles
    - Requisitos de protección física
    - Las restricciones para la instalación de software
    - Aplicación de actualizaciones y parches del software
    - Restricción a la conexión de servicios de información
    - Control de acceso
    - Protección contra software malicioso
    - Des habilitación remota, borrado o cierre.
    - Respaldos
    - Uso de servicios y aplicaciones web

Se deberá tener cuidado cuando: el uso de dispositivos móviles en lugares públicos, salas de reunión y áreas no protegidas, adicional se deberá tener protección para evitar el acceso o divulgación no autorizada de la información almacenada y procesada.

Para el uso de dispositivos móviles de propiedad personal se debe considerar las siguientes políticas y medidas:

- La separación entre el uso privado y el uso por trabajo, incluir el uso de software para apoyar la separación y proteger los datos de la organización.
- Para conceder acceso a la información de la organización los usuarios deberán firmar un acuerdo de usuario final para: protección física, aplicación de actualizaciones necesarias, desistir de la información de la organización, permitir el borrado remoto de datos en caso de robo o pérdida del dispositivo, adicional se tendrá en cuenta la legislación sobre la privacidad.

✓ **Teletrabajo**

Control

Se deberá implementar una política y medidas de seguridad que den soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares donde se realiza teletrabajo.

Guía de implementación

La política define las condiciones y restricciones para el teletrabajo. Se deben tener en cuenta los siguientes puntos cuando se considere aplicable y permitido:

- La seguridad física existente en el sitio de teletrabajo, la edificación y el entorno local.
- Requisitos para la seguridad en las comunicaciones, tomando en cuenta la necesidad de conexión remota a los sistemas

internos de la organización, la sensibilidad de los datos a través del enlace de comunicación.

- La amenaza de acceso no autorizado a los datos o recursos, por parte de otras personas, familia o amigos que habitan en la misma edificación.
- Configuraciones necesarias en el uso de redes inalámbricas en redes domésticas.
- Verificar la seguridad del equipo de cómputo de propiedad privada.
- Controlar requisitos de firewall y de protección contra software malicioso.
- Suministrar de equipos y dispositivos de almacenamiento para las actividades de teletrabajo, en el caso que no se permita el uso de equipos de propiedad privada y que no están bajo control de la organización.
- Determinar, el trabajo permitido, horas de trabajo, información clasificada que se puede mantener, y sistemas autorizados durante el teletrabajo.
- Devolución de los equipos, revocación de accesos y autorizaciones una vez que finalice el periodo de teletrabajo.

- **Durante el empleo**

  Objetivo: asegurar que los empleados tomen conciencia de sus responsabilidades en torno a la seguridad de la información y sean cumplidas.

- ✓ **Sensibilización, educación y formación en materia de seguridad de la información**

  Control

  Todos los empleados de la organización deberán recibir la educación y formación, actualizaciones regulares y procedimientos sobre la seguridad de información pertinentes a su cargo.

  Guía de implementación

  Implementación de un programa de toma de conciencia en seguridad de la información en línea con las políticas y procedimientos de la organización. Las campañas de concientización deberán tener varias actividades como por ejemplo “día de la seguridad de la información” con la elaboración de folletos y boletines.

  La formación en seguridad de la información también deberá comprender los siguientes aspectos de manera general:

  - El compromiso de la dirección con la seguridad de la información de toda la organización.
  - Es necesario la familiarización con las reglas y obligaciones de seguridad de la información aplicables y cumplir con ellas.
  - Aplicación de procedimientos básicos de seguridad de la información tales como: reporte de incidentes, seguridad en las contraseñas, controles contra software malicioso y escritorios limpios.

  La educación y la formación en seguridad de la información se deberá realizar de forma periódica, antes de la activación del rol en caso de nuevo personal o cambio de puesto se deberá realizar el entrenamiento inicial donde se enmarquen los cargos, roles y requisitos de seguridad de la información.

Información adicional

En la preparación del programa es importante no solo enfocarse en el “que”, también en el “como” y “por qué”, lo cual es muy importante para que el empleado comprenda el objetivo de la seguridad de la información y el impacto potencial.

Se deberá llevar a cabo una valoración a través de una evaluación de la compresión de los empleados al finalizar el programa de formación.

- ✓ **Cese o cambio responsabilidades laborales**

Control

Las responsabilidades y deberes que permanecen validos en cuanto a la seguridad de la información, después de terminar o cambio de contrato deberán ser definidos, comunicar y hacer cumplir al empleado.

Guía de implementación

La comunicación oportuna de las responsabilidades en la terminación o cambio se deberá incluir en los requisitos regulares de la seguridad de la información y las responsabilidades legales, las cuales deben constar en un acuerdo de confidencialidad, términos y condiciones del contrato, que continúan vigentes luego de finalizar el contrato del empleado.

Para los cambios de responsabilidad o de empleador, se deberá manejar como una terminación de un contrato actual y combinada con el inicio de un nuevo contrato y sus responsabilidades.

Información adicional

El proceso de recursos humanos generalmente es el responsable de la gestión de terminación del contrato, y deberá trabajar junto al coordinador o jefe de la persona que sale para gestionar los aspectos de seguridad de la información relevantes.

- **Responsabilidad de los activos**

Objetivo: identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.

- ✓ **Inventario de activos y otros activos asociados**

Control

Se deberá identificar los activos asociados con la información y las infraestructuras de procesamiento de información, para lo cual se debe procesar y mantener un inventario de los activos.

Guía de implementación.

La organización deberá identificar los activos pertinentes en el ciclo de vida de la organización, documentar su importancia; para el ciclo de vida de la información debe incluir: creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción.

El inventario de activos deberá ser exacto, mantenerse actualizado y alineado a los otros inventarios.

Para cada activo identificado, se deberá asignar un responsable del activo y su clasificación.

Información adicional

Los inventarios de activos aseguran que se cuenta con una protección efectiva, y tienen otros propósitos, razones de salud y seguridad, seguros o asuntos financieros.

Control

Los activos mantenidos deben tener un responsable.

Guía de implementación

El responsable del activo deberá gestionarlo apropiadamente durante el ciclo de vida del mismo.

El responsable del activo deberá:

- Asegurarse de que los activos a su cargo estén inventariados
- Asegurarse que los activos estén clasificados y protegidos apropiadamente.
- Revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes, tomando en cuenta las políticas de control aplicadas.
- Asegurar el manejo adecuado del activo cuando es eliminado o destruido.

Información adicional

El responsable identificado puede ser un individuo o un proceso que tenga la responsabilidad de gestionar apropiadamente el ciclo de vida del activo. Adicional no tiene ningún derecho de propiedad sobre el activo.

- ✓ **Uso aceptable de activos**

  Control

  Se deberá identificar, documentar e implementar reglas del uso aceptable de la información y activos asociados e infraestructura de procesamiento de información.

  Guía de implementación

  Los empleados que usan los activos de la organización deben tomar conciencia sobre los requerimientos necesarios de la seguridad de información, como también serán los responsables del uso que hacen de cualquier recurso, proceso de información, y de cualquier uso ejecutado bajo su responsabilidad.

- ✓ **Devolución de activos**

  Control

  Todos los empleados deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

  Guía de implementación

  El proceso de terminación debe formalizar la devolución de todos los activos físicos y electrónicos que hayan sido entregado, que son de propiedad de la organización o fueron confiados a ella.

  En caso de que un empleado posea conocimientos que son importantes para las diferentes operaciones, esa información se deberá documentar y transferir a la organización.

  Durante el periodo de entrega o terminación del puesto de trabajo, la organización deberá controlar el copiado, eliminación, no autorizada de la información pertinente por parte del empleado.

- **Clasificación de la información**

  Objetivo: asegurar que la información tenga un nivel adecuado de protección, de acuerdo a la importancia para la organización.

  - ✓ **Clasificación de la información**

    Control

    La información deberá ser clasificada en función de: requisitos legales, valor, criticidad y susceptibilidad a divulgación o a ser modificada de manera no autorizada.

    Guía de implementación

    Las clasificaciones y controles de protección a la información deberán tomar en cuenta las necesidades del negocio, intercambio o restricción de información, los dispositivos o activos que almacenen información también se pueden clasificar de conformidad con la información en el activo.

    Los responsables de los activos de información o dispositivos de almacenamiento deben rendir cuantas por su clasificación.

    El esquema de clasificación deberá estar alineado al nivel de protección donde se valorará analizando la confidencialidad, la integridad y la disponibilidad. Cada nivel deberá recibir un nombre que tenga sentido en el contexto de aplicación.

    Información adicional

    La información puede dejar de ser reservada o critica después de un lapso de tiempo, como por ejemplo cuando la información ya se ha hecho pública.

    Un ejemplo de cómo se podría esquematizar la clasificación de la información de acuerdo a su confidencialidad, se basaría en los siguientes niveles:

- La divulgación no causa peligro
- La divulgación causara un inconveniente operativo menor
- La divulgación tendrá un impacto a corto plazo en las operaciones u objetivos
- La divulgación tendrá un impacto serio en los objetivos estratégicos a largo plazo o pone en riesgo la supervivencia de la organización

✓ **Etiquetado de la información**

Control

Desarrollar e implementar de manera adecuada un conjunto de procedimientos para etiquetar la información, de acuerdo a su clasificación revisada y adoptada por la organización.

Guía de implementación

El etiquetado de la información necesita procedimientos abarcaran la información y activos relacionados en formatos físicos y electrónicos. El etiquetado reflejara la clasificación de la información revisando en el punto anterior.

Las etiquetas deben ser de fácil reconocimiento, el procedimiento para la colocación de las etiquetas debe ser claras en donde y como se colocan dependiendo del tipo de activo, dispositivo o medio.

Los procedimientos pueden indicar donde se puede omitir el etiquetado por ejemplo para la información no confidencial.

Información adicional

El etiquetado de información y su clasificación debe ser un requisito clave para el intercambio de información.

Algunas veces existen efectos negativos en el etiquetado de la información, porque los activos clasificados son más fáciles de identificar y ser hurtados por atacantes internos o externos.

- ✓ **Uso aceptable de la información y otros activos asociados.**

  Control

  Desarrollar e implementar procedimientos para el manejo de información y los activos, de acuerdo al esquema de clasificación.

  Guía de implementación

  Redactar procedimientos para el manejo, procesamiento, almacenamiento y transferencia de la información de conformidad con la clasificación a la que pertenece.

  Considerar los siguientes puntos:

  - Cada nivel de clasificación dependerá de las restricciones de acceso que soportan.
  - Mantener un registro formal de los activos y sus receptores autorizados.
  - Protección de copias de información temporal o permanente y que tenga coherencia con la información original.
  - Los activos deben ser almacenados de acuerdo a las especificaciones de los fabricantes.
  - El etiquetado claro de todas las copias o respaldos para fácil identificación por el receptor autorizado.

  El intercambio de información con otras organizaciones deberá incluir procedimientos para la identificación y clasificación para la correcta interpretación de otras etiquetas ajenas a la organización.

- **Manejo de los medios de almacenamiento**

  Objetivo: evitar la circulación, modificación, retiro o destrucción no autorizados de información almacenada en los medios.

  - ✓ **Medios de almacenamiento**

    Control

    Implementar procedimientos para gestionar los medios removibles, de acuerdo al esquema de clasificación de la información adoptada por la organización.

    Guía de implementación

    Considerar las siguientes normas para gestionar los medios removibles:

    - Al no requerir el contenido de cualquier medio reusable y que se vaya a retirar de la organización, se deberá remover de forma que no se recuperable.
    - Se deberá llevar un registro de donde se indique la autorización para retirar dichos medios de la organización.
    - Todos los medios de almacenamiento se deberán resguardar en un ambiente protegido y seguro.
    - Si la información almacenada en los medios removibles es de confidencialidad o integridad, se deberán usar técnicas criptográficas para proteger los datos.
    - Se deberá guardar varias copias de los datos valiosos en medios separados, con ellos se reducirá el riesgo de daño o perdida.
    - Considerar el registro de los medios removibles para reducir la probabilidad de perdida de datos.

    Se deben documentar los procedimientos y niveles de autorización.

Control

Utilizar procedimientos formales para disponer en forma segura de los medios de almacenamiento cuando ya no se requieran.

Guía de implementación

Los procedimientos para la práctica segura de los medios de almacenamiento los cuales contienen información confidencial deberán estar conformes al nivel de sensibilidad de la información.

Tomar en cuenta los siguientes puntos:

- Los medios de almacenamiento que contienen información de gran importancia se deberán almacenar y dispone de forma segura: destrucción o borrado de los datos antes de ser usado por otro proceso dentro de la organización.
- Se recomienda organizar los medios de almacenamiento al recolectarlos y disponer de ellos de manera segura, que intentar segregarlos de los elementos críticos.
- Se debe mantener un registro de aquellos elementos o medios de almacenamiento críticos.

Información adicional

Aquellos dispositivos o medios de almacenamiento dañados que contienen datos sensibles, se deberá medir el riesgo para determinar si es necesaria la destrucción total físicamente o enviarlos a reparación u desecharlos.

Control

Aquellos medios de almacenamiento que contengan información deberán tener seguridad contra los accesos no autorizados, el uso indebido o corrupción durante el transporte.

Guía de implementación

Los siguientes puntos se deben considerar para la asegurar la protección de la información durante el transporte.

- Usar transportes o servicios de mensajería confiables
- Tener un acuerdo dentro de la organización con la lista autorizada que de servicios de mensajería.
- Procedimientos para verificar e identificar los servicios de mensajería.
- El embalaje o resguardo físico durante el trasporte deberá asegurar que el contenido se mantenga en perfectas condiciones hasta que sea entregado a su destinatario.
- Registrar e identificar el contenido de los medios, al igual que tiempos de entrega, responsables durante el transporte y el recibido por parte del destinatario.

Información adicional

En el caso que la información contenida en los medios de almacenamiento no se encuentre encriptada, considerar una protección física adicional.

- **Requisitos empresariales del control de acceso**

Objetivo: limitar mediante procedimientos el acceso a la información e infraestructuras donde se procesa información.

- ✓ **Control de acceso**

  Control

  Establecer, documentar y revisar la normativa de control de acceso en base en los requisitos y seguridad de la información.

  Guía de implementación

  Las indicaciones claras en cuanto a requisitos y control de acceso se deben hacer cumplir a cada uno de los usuarios.

  La normativa debe tener en cuenta lo siguiente.

  - Requisitos de seguridad para las aplicaciones de la organización
  - Debe haber coherencia entre los accesos autorizados y el esquema de clasificación de los sistemas y redes.
  - Gestión de controles de acceso en un entorno distribuido y en red, donde se identifique todos los tipos de conexión disponible.
  - Debe existir una separación en los roles de control de acceso, es decir para solicitudes, autorizaciones y administración de accesos.
  - Debe existir revisiones periódicas en las solicitudes, requisitos y retiros de controles de acceso.
  - Mantener un registro de los usuarios y sus accesos de los diferentes eventos significativos e información de autenticación secreta.
  - Roles de acceso privilegiado

  Información adicional

  Se debe considerar los siguientes puntos.

  - Establecer normas basadas en la premisa “En general, todo está prohibido, a menos que se permita expresamente”, y no en la menos estricta: “En general, todo está permitido, a menos que se prohíba expresamente”

- Tener en cuenta las normas que requieres aprobación especifica antes de su puesta en marcha y las que no requieren aprobación

Dos principios que dirigen la normativa de control de acceso son:

- Lo que necesita conocer: solo conceder acceso a la información necesaria para que el usuario realice sus tareas.
- Lo que necesita usar: solo puede acceder a la infraestructura de procesamiento de información, que el usuario necesita para realizar sus tareas.

- **Gestión de acceso de los usuarios.**

Objetivo: asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a los sistemas y servicios.

- ✓ **Registro y baja de usuarios**

Control

Se deberá incorporar un procedimiento formal de registro o activación, y de cancelación o des habilitación del registro de usuarios, con lo cual se posibilita la asignación de normas de acceso.

Guía de implementación

El procedimiento para mantener la identificación de usuarios debe incluir:

- Aplicar identificaciones únicas por cada usuario, los cuales estarán vinculados a las acciones y responsabilidades correspondientes.
- Se deberá permitir el uso de identificaciones compartidas solo cuando sea necesario por motivos de operación o que permita la organización y deberá ser aprobada y documentada.

- Deshabilitar o retirar inmediatamente las identificaciones de los usuarios que han dejado la organización.
- Identificar y deshabilitar o a su vez eliminar las identificaciones de usuarios redundantes y estos usuarios no sean asignados a otros usuarios.

Información adicional

El suministrar o revocar el acceso a la información a la infraestructura de procesamiento de información se procede en dos pasos:

- Asignación y habilitación, o deshabilitar la identificación del usuario.
- Activar o deshabilitar los derechos de acceso al usuario.

✓ **Derechos de acceso**

Control

Se debe implementar un procedimiento de entrega de acceso formal de usuarios con lo cual se podrá asignar o deshabilitar los accesos a todo tipo de usuarios en todos los sistemas y servicios.

Guía de implementación

El procedimiento para la entrega de acceso que servirá para activar o deshabilitar los accesos otorgados a las identificaciones de usuarios debe incluir:

- Tener la apropiada aprobación de derechos de acceso por parte del coordinador o jefe inmediato, con lo cual el propietario del sistema de información autorizara el acceso para el uso de sistemas y servicios de información.
- Mantener un registro central de las normas de acceso dadas a cada cuenta de usuario para el uso de sistemas de información y servicios.
- Para los casos de cambio de rol de usuario adaptar las normas de acceso correspondientes al nuevo proceso y en

los casos que el usuario deje la organización, retirar o bloquear de manera inmediata las reglas de acceso a sistemas de información y servicios.

Información adicional

Se debe considerar el incluir en los contratos del personal y en los contratos de los diferentes servicios, numerales específicos de sanciones en casos de intentos de acceso no autorizados.

- ✓ **Derecho de acceso privilegiado**

Control

Se debe restringir y controlar las asignaciones y autorizaciones de acceso privilegiado.

Guía de implementación

Las asignaciones y autorizaciones de acceso privilegiado deben tener un control formal del proceso de autorización.

- En necesario la identificación de las reglas de acceso privilegiado que corresponden a cada sistema o proceso, aplicaciones y usuarios que necesiten la asignación, ejemplo: sistema operativo, gestión de base de datos.
- Las reglas de acceso privilegiado se deberán asignar a los usuarios en base a los requerimientos mínimos para sus funciones correspondiente al rol que desempeñen y la necesidad de uso por cada caso.
- Se debe revisar con más frecuencia las asignaciones y controles de acceso privilegiados para asegurar no se hayan obtenido privilegios no autorizados adicional se debe registrar todo cambio realizado a las cuentas de usuario.
- Para el uso de reglas de acceso privilegiado se deberán asignar un usuario o identificación diferente a la usada para las actividades regulares.

Información adicional

El uso indebido de los privilegios del sistema administrado es un factor que contribuye a fallas o violaciones a los sistemas.

- ✓ **Información de autenticación**

  Control

  Mediante un proceso de gestión formal se deberá controlar la asignación de información de autenticación secreta.

  Guía de implementación

  El proceso deberá contener los siguientes requisitos:

  - Se debe solicitar a los usuarios que firmen una declaración de confidencialidad de la información de autenticación secreta de usuario al igual que la de grupo en caso que sea compartida solo para los miembros del grupo, esta declaración se podría incluir en los términos y condiciones del empleo.
  - Al solicitar al usuario que mantenga su información de autenticación secreta, se le deberá proporcionar accesos temporales y obligar al cambio en el primer uso.
  - Se debe establecer un procedimiento de verificación de identidad de un usuario antes de generar y proporcionar nueva información de autenticación secreta temporal o reemplazo.
  - Se deberá suministrar a los usuarios de manera segura la información de autenticación secreta, se debe evitar uso de partes externas o de mensajes de correo electrónico no protegidos.
  - La información de autenticación secreta por defecto o del fabricante, deberá ser modificada después de la instalación del sistema o software.

Información adicional

Son tipos de información de autenticación secreta: las contraseñas usadas comúnmente, llaves criptográficas y otros datos almacenados en tokens de hardware que producen códigos de autenticación.

- **Control de acceso al sistema y a las aplicaciones**

Objetivo: evitar el ingreso no autorizado a sistemas y aplicaciones.

- ✓ **Restricción de acceso a la información**

Control

En conformidad a la política de control de acceso se deberá restringir el ingreso a la información y a las funciones del sistema de las aplicaciones.

Guía de implementación

Considerar los siguientes puntos como soporte para la restricción de acceso:

- Hacer uso de menús para mantener el control de acceso en los diferentes sistemas de tipo aplicación.
- Controlar a que datos puede tener acceso y las reglas sobre ellos, lectura, escritura o ejecución, borrado o eliminación.
- Administrar controles de acceso físico o lógico para el aislamiento de las aplicaciones o sistemas críticos.

- ✓ **Autenticación segura**

Control

En el caso que la política de control de acceso lo requiera se deberá controlar mediante un procedimiento de ingreso seguro.

Guía de implementación

En los casos donde se requiera una verificación de identificación fuerte, se deberá usar métodos de autenticación alternativos a las

comunes, podría ser medios criptográficos, tarjetas inteligentes, tokens o medios biométricos.

Se debe diseñar un proceso para el ingreso a un sistema o aplicación, para disminuir la probabilidad de acceso no autorizado.

El proceso de ingreso seguro deberá incluir:

- Mediante una notificación visual advertir de manera general que solo los usuarios autorizados pueden acceder al computador.
- Evitar el uso de mensajes de ayuda durante el proceso de ingreso.
- Se deberá validar el ingreso solamente cuando todos los datos de entrada estén completos, al dar un error, el sistema no debe indicar que parte de los datos es incorrecta.
- Protección contra ingresos de fuerza bruta.
- Se debe registrar los intentos exitosos y fallidos.
- Al terminar el ingreso seguro se debe visualizar la siguiente información:
  1) Fecha y hora de ingreso previo exitoso.
  2) Detalles de cualquier intento fallido desde el ultimo ingreso exitoso.
- Mantener oculta la contraseña que se esté ingresando
- Evitar la trasmisión de contraseñas en texto claro por la red
- Terminar sesiones inactivas después de un tiempo determinado de inactividad.
- Tener restricciones en los tiempos de conexión para añadir seguridad en las aplicaciones y sistemas de alto riesgo y evitar la ventana de acceso no autorizado.

Información adicional

La fortaleza de autenticación del usuario debe ser apropiado o proporcional a la clasificación de la información a la que va a acceder.

Al transmitir contraseñas en texto claro durante la sesión de ingreso a la red, pueden ser fácilmente capturadas por programas "*sniffer*" de redes.

- ✓ **Sistema de gestión de contraseñas**

  Control

  El sistema de gestión de contraseñas, debe ser interactivos y asegurar la calidad de las mismas.

  Guía de implementación

  - Uso obligatorio de usuarios y contraseñas individuales.
  - Permitir a los usuarios que seleccionen y cambien sus propias contraseñas e incluir un proceso de confirmación.
  - Exigir la selección de contraseñas de calidad.
  - Forzar el cambio de contraseña en el primer ingreso
  - Exigir cambios de contraseñas de forma regular.
  - Se debe llevar un registro de contraseñas usadas anteriormente e impedir su uso.
  - Se debe mantener oculta la contraseña cuando se esté digitando en pantalla.
  - Almacenar los datos de las contraseñas separados de los datos de las aplicaciones.
  - Almacenar y transmitir las contraseñas de forma segura.

- ✓ **Uso de programas de utilidad privilegiados**

  Control

  Se debe limitar y controlar estrictamente el uso de programas utilitarios que puedan tener la capacidad de anular los sistemas y los controles de las aplicaciones.

  Guía de implementación

  Para el uso de programas utilitarios se deberá considerar las siguientes directrices:

  - Procesos de identificación, autenticación y autorización para el uso de programas utilitarios.
  - Separar los programas utilitarios del software de aplicaciones.
  - Limitar el uso de programas utilitarios a un número mínimo de usuarios confiables y autorizados.
  - Registro del uso de los programas utilitarios.
  - Definir y documentar los niveles de autorización por programa utilitario.
  - Retirar o inhabilitar todos los programas utilitarios innecesarios.
  - No colocar a disposición los programas utilitarios o usuarios que tengan acceso a los sistemas y donde se requiera la separación de responsabilidades.

- ✓ **Acceso al código fuente**

  Control

  Restringir el acceso a los códigos fuentes de los programas.

  Guía de implementación

  Se debe controlar estrictamente los accesos a los códigos fuente a los programas y elementos asociados como, diseños, especificaciones, planes de validación y verificación, con el fin de evitar cambios o introducción de funcionalidad no autorizadas y mantener la confidencialidad.

Se debe considerar los siguientes puntos para el control de acceso a los códigos fuente:

- En lo posible no se debe mantener las librerías de fuentes de programas en los sistemas operativos.
- Los códigos y librerías de fuentes de los programas se deben gestionar de acuerdo a los procesos y procedimientos establecidos.
- Debe tener restricción de acceso al código fuente el personal de soporte.
- Las actualizaciones de librerías de fuentes y elementos asociados, y la entrega de fuentes de programas solo se deberá hacer una vez que se haya autorizado apropiadamente.
- Mantener en un entorno seguro los listados de programas.
- Se debe mantener el registro de auditoría de todos los accesos a las librerías de fuente de programas.
- Si los códigos fuente están listos para publicación se debe considerar controles adicionales para asegurar su integridad.

- **Controles criptográficos**

Objetivo: certificar el uso apropiado y fuerte de la criptografía para la protección de la confidencialidad, autenticidad y/o integridad de la información.

- ✓ **Uso de la criptografía**

  Control

  Se debe desarrollar e implementar reglas sobre el uso de controles criptográficos para la protección de la información.

  Guía de implementación

  Para el desarrollo de reglas sobre el uso de criptografía se recomienda:

  - En base a la valoración de riesgos, se debe identificar el nivel de protección requerida, tomando en cuenta el tipo de fortaleza y calidad del algoritmo de encriptación requerido.
  - Se debe usar la encriptación para la protección de la información transportada por dispositivos móviles o removibles, o transmitida a través de líneas de comunicación.
  - Manejar la gestión de llaves, incluir la protección de llaves criptográficas y la recuperación de información encriptada, en los casos de pérdida o daño de llaves cuya seguridad están comprometidas.
  - Roles y responsabilidades, ejemplo:
    1) Responsable de la implementación de las reglas
    2) Responsable de gestión de llaves y la generación de las mismas
  - Reglas que se van a adoptar para una implementación efectiva en las organizaciones.

  Los controles criptográficos pueden ser usados para cumplir diferentes objetivos de seguridad de información:

  - Confidencialidad: para proteger información sensible o critica, que sea almacenada o transportada.
  - Integridad/autenticidad: uso de códigos de autenticación o firmas digitales para comprobar la autenticidad o integridad de la información.

- No-repudio: proporcionar evidencia de que un evento ocurrió o no.
- Autenticación: autenticación de usuarios o entidades que solicitan acceso a los sistemas.

- **Zonas seguras**

Objetivo: prevenir el acceso físico no autorizado, el perjuicio o daño, interferencia a la información y a la infraestructura de procesamiento de información en las organizaciones.

- ✓ **Parámetros de seguridad física.**

Control

Se debe realizar y poner en uso parámetros de seguridad, para proteger aquellas áreas que contengan información sensible o crítica e infraestructura que maneja la información.

Guía de implementación

Se debe considerar e implementar los siguientes parámetros de seguridad física:

- Se debe definir los perímetros de seguridad, la localización y la fortaleza de cada uno, lo cual dependerá de los requisitos de seguridad de los activos dentro del perímetro y los resultados de la valoración de riesgos.
- Los perímetros de la edificación o lugar que contenga infraestructura de procesamiento de la información deberá ser físicamente seguros, el techo exterior, las paredes y el material de los pisos del sitio deberían ser de construcción sólida, y todas las paredes externas deberían estar protegidas adecuadamente contra acceso no autorizado con mecanismos de control (por ejemplo, barras, alarmas, cerraduras); las puertas y ventanas deberían estar cerradas con llave cuando no hay supervisión, y se debería considerar

protección externa para ventanas, particularmente al nivel del suelo.

- El acceso al sitio o lugar debe estar restringido únicamente para personal autorizado.
- Se debe instalar o adecuar sistemas para la detección de intrusos todo de acuerdo a normativas de cada organización.
- Las infraestructuras de procesamiento de información gestionadas por las organizaciones deben estar físicamente separadas de las gestionadas por externos.

✓ **Entrada física**

Control

Toda área segura se deberá proteger mediante el uso de controles de ingreso apropiados para así asegurar que solamente se permite el acceso a personal autorizado.

Guía de implementación

Se debe considerar los siguientes puntos:

- Llevar un registro con fecha y hora de ingreso y salida de usuarios, todos deben ser supervisados a menos que su acceso haya sido aprobado previamente, y debe ser acceso para propósitos específicos. La identidad de los usuarios se debe autenticar por medios apropiados.
- Las áreas que procesan o almacenan información confidencial se deberá restringir solo a usuarios autorizados con la implementación de controles apropiados, ejemplo: tarjeta de acceso o un pin secreto.
- Se debe mantener y realizar seguimiento del libro de registro o logs generados como rastro de auditoria electrónica de todos los accesos.

- ✓ **Asegurar las oficinas, salas e instalaciones.**

  Control

  Diseñar y aplicar seguridad física en oficinas, salas e instalaciones.

  Guía de implementación

  Se debe considerar las siguientes directrices:

  - Las instalaciones importantes deben ser ubicadas de manera que se impida el acceso al público.
  - Las instalaciones e edificaciones deben ser discretas y dar un indicio mínimo del propósito.
  - La configuración de las instalaciones debe evitar que las actividades sean visibles y audibles desde el exterior.

- ✓ **Protección contra las amenazas físicas y medioambientales.**

  Control

  Se debe diseñar y aplicar seguridad física con las diferentes amenazas: desastres naturales, ataques maliciosos o accidentes.

  Guía de implementación

  - En el plan de mitigación de riesgos debe presentar las diferentes amenazas que presentan las instalaciones e infraestructuras donde se procesa la información.
  - Contar con recursos y asesoría técnica especializada para mitigar cada uno de los riesgos descubiertos en la matriz.

- ➢ **Seguridad en equipos.**

  Objetivo: Prevenir el daño, robo, perdida de activos, y la interrupción de operaciones de la organización.

  - ✓ **Ubicación y protección de los equipos**

Control

Los equipos deberán estar protegidos y ubicados para la reducción de riesgos de amenazas, peligros del entorno, y evitar las oportunidades de acceso no autorizado.

Guía de implementación

Se debe tomar en consideración las siguientes directrices para la protección de los equipos:

- Ubicar los equipos de manera que se disminuya el acceso innecesario a las áreas de trabajo.
- Las estructuras de procesamiento de información que manejen datos sensibles deben estar ubicados cuidadosamente para disminuir el riesgo de que personas no autorizadas puedan ver la información durante su uso.
- Los dispositivos y equipos de almacenamiento se deberán asegurar para evitar el acceso no autorizado.
- Se deben adoptar controles para minimizar los riesgos de amenazas físicas y ambientales, por ejemplo, robo, incendio, explosivos, humo, agua (fallas en el suministro de agua), polvo, vibraciones, efectos químicos, interferencia en el suministro eléctrico, interferencia en las redes de comunicación, radiación electromagnética y vandalismo.
- Establecer directrices sobre el comer, consumir líquidos y fumar cerca de las estructuras de procesamiento de información.
- Realizar seguimientos de las condiciones ambientales como: temperatura y humedad, para determinar condiciones que pueden afectar adversamente las estructuras de procesamiento de información.
- La protección contra descargas eléctricas atmosféricas se debe aplicar en todas las edificaciones y se debe colocar

filtros en todas las líneas de redes de comunicación y de potencia entrantes, para la protección de dichas descargas.

- Considerar el uso de métodos de protección especial, tales como membranas para teclados, para equipos en ambientes industriales.

✓ **Seguridad del cableado**

Control

Los cableados de potencia y telecomunicaciones que soporta servicios de información deben estar protegido contra interceptación, interferencia o daño.

Guía de implementación

Considerar las siguientes directrices para seguridad del cableado:

- Las líneas de potencia y de telecomunicaciones que ingresan a las estructuras de procesamiento de información deben ser subterráneas donde sea posible, o tomar en cuenta protección alternativa adecuada.

Los cables de potencia deben estar separados de los cables de comunicación para evitar interferencias.

En el caso de sistema sensibles o críticos considerar la inclusión de los siguientes controles adicionales:

- La instalación de Conduit apantallado y cajas con llave en los puntos de inspección.
- Usar blindaje electromagnético para protección del cableado.
- Dar inicio de barridos técnicos e inspecciones físicas a dispositivos no autorizados que se conectan a los cables.

✓ **Mantenimiento de equipos**

Control

Se deberán mantener correctamente los equipos para asegurar su disponibilidad e integridad continua.

Guía de implementación

Considerar las siguientes directrices para el mantenimiento de equipos:

- Los equipos se deben mantener de acuerdo a los intervalos y especificaciones de servicio recomendados por el proveedor.
- Solo personal autorizado de mantenimientos deberá llevar a cabo las reparaciones y dar servicio a los equipos.
- Llevar un registro de todas las fallas reales y sospechosas, y de todo mantenimiento preventivo y correctivo.
- Implementar controles apropiados cuando el equipo está programado para el mantenimiento, tomando en cuenta si este lo lleva a cabo el personal en el sitio o personal externo a la organización; donde sea necesario, la información confidencial debe ser borrada del equipo, o el personal de mantenimiento deberá retirarse lo suficiente de la información.
- Antes de volver a colocar el equipo en operación, después del mantenimiento, debe ser inspeccionado para asegurar que no ha sido alterado y que el funcionamiento es el adecuado.

✓ **Seguridad de los activos fuera de las instalaciones**

Control

Aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, tomando en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.

Guía de implementación

El uso de cualquier equipo / dispositivo de almacenamiento o procesamiento de información por fuera de las instalaciones debe ser aprobado por la dirección. Esto aplica a activos de propiedad de la organización y a activos de propiedad privada que son usados a nombre de la organización.

Se debe considerar los siguientes puntos para proteger los equipos fuera de las instalaciones:

- Los activos y medios retirados de las instalaciones no se deberán dejar sin vigilancia en lugares públicos.
- Los controles en lugares fuera de las instalaciones, como trabajo en casa, teletrabajo y sitios temporales se deberán determinar mediante una valoración de riesgos y aplicar los controles adecuados según sean apropiados, por ejemplo, gabinetes de archivo con llave, política de escritorio despejado, controles de acceso para computadores y comunicación segura con la oficina.
- En el caso de que el activo fuera de las instalaciones es transferido entre diferentes individuos y partes externas, se deberá llevar un registro que defina la cadena de custodia para el activo, este debe incluir al menos los nombres y las áreas o procesos de los responsables del equipo.

Información adicional

El activo de procesamiento y almacenamiento de información incluye todas las formas de computadores personales, organizadores, teléfonos móviles, tarjetas inteligentes, papel u otro formato, que se mantenga para trabajo en la casa o que se transporte lejos del lugar de trabajo normal.

- ✓ **Eliminación segura y reutilización de equipos.**

Control

Se debe verificar todos los elementos del activo que contenga medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su eliminación o reusó.

Guía de implementación

Antes de su eliminación o reusó, se debe verificar que los equipos no contengas el medio de almacenamiento.

Los medios o dispositivos de almacenamiento que contienen información confidencial o protegida por derechos de autor se deberán destruir físicamente, eliminar o sobrescribir usando técnicas para hacer que la información original no sea recuperable, en vez de usar la función estándar borrar o formatear.

Información adicional

Los equipos o dispositivos dañados que contienen o son medios de almacenamiento pueden requerir una valoración de riesgos para determinar si los elementos se deben destruir físicamente en vez de enviarlos a reparación o desecharlos. La información puede ser comprometida debido a una disposición descuidada o reúsos de equipos.

También el asegurar el borrado de discos, la encriptación del disco entero reduce el riesgo de que se divulgue información confidencial o critica cuando se dispone del equipo o es destinado para otros factores, siempre y cuando:

- El proceso de encriptación debe ser lo suficientemente fuerte y abarque todo el disco (incluido el espacio perdido, archivos temporales de intercambio, etc.)
- Las contraseñas de encriptación deben ser lo suficiente largas para resistir ataques de fuerza bruta.
- Las contraseñas de encriptación deben mantenerse confidenciales (nunca se almacenen en el mismo disco)

- ✓ **Dispositivos de punto final del usuario**

  Control

  Los usuarios deberán asegurarse que los equipos desatendidos se les dé una protección apropiada.

  Guía de implementación

  Cada uno de los usuarios debe tomar conciencia de los requisitos y procedimientos de seguridad para proteger los equipos desatendidos, y aplicar sus responsabilidades para la aplicación de la protección.

  Se notificará a los usuarios que:

  - Cerrar las sesiones activas cuando hayan terminado, a menos que se puedan asegurar mediante mecanismos de bloqueo apropiados, ejemplo: protector de pantalla con contraseña.
  - Salir de las aplicaciones y servicios de red cuando ya no los necesiten.
  - Asegurar computadores y dispositivos móviles contra uso no autorizado, ejemplo acceso con contraseña, cuando no esté en uso.

- ✓ **Escritorio y pantalla despejados**

  Control

  Se debe adoptar la política de escritorio y pantalla despejados, para los papeles y medios de almacenamiento removibles, en la infraestructura de procesamiento de información.

  Guía de implementación

  La política de escritorio y pantalla despejados, de be tener en cuenta la clasificación de la información (véase literal e), riesgos y aspectos culturales correspondientes a la organización. Tomar en cuenta las siguientes directrices:

La información sensible o critica de la organización, papeles, medios de almacenamiento electrónico, debe guardarse bajo llave (muebles o gabinete de seguridad) cuando no se requiera, especialmente cuando la oficina este desocupado.

- Los computadores y terminales se deberán dejar fuera del sistema o protegidos con sistema de bloquee de pantalla y teclado, control por contraseña, token o mecanismos similares para la autenticación del usuario.

Información adicional

La política de escritorio y pantalla despejados reduce los riesgos de acceso no autorizado, perdida o daño de información durante y fuera de horas laborales normales. Los muebles o gabinetes de seguridad podrían proteger la información almacenada en casos como: incendios, terremotos, inundaciones o explosión.

- **Protección contra el malware.**

Objetivo: asegurar que la información y la infraestructura de procesamiento de información se mantengan protegidas contra malware.

- ✓ **Controles contra el malware**

Control

Se debe implementar control de detección, prevención y recuperación, combinados con la toma de conciencia apropiada de los usuarios, para protección contra el malware.

Guía de implementación

La protección contra el malware se debe basar en software de detección y de recuperación, toma de conciencia sobre la seguridad de la información, y mantener los controles apropiados en la gestión de cambios y acceso al sistema, tomar en consideración las siguientes directrices:

- Establecer una política formal que prohíba el uso de software no autorizado.
- Implementación de controles para evitar y detectar el uso de software no autorizado. Ejemplo: lista blanca de aplicaciones.
- Implementación de controles para evitar y detectar el uso de sitios web maliciosos o sospechosos.
- Establecer una política formal contra los riesgos asociados a la obtención de software a través de redes externas o de otro medio, donde se indique las medidas externas que se deben tomar.
- Reducir las vulnerabilidades mediante la gestión técnica, para que el malware no pueda aprovecharlas.
- Organizar y aplicar revisiones regulares de software y del contenido de los datos del sistema que apoyan en los procesos críticos de la organización, investigar la presencia de software y archivos no aprobados y no autorizados.
- La instalación y actualización regular de software de detección y reparación de malware, en los computadores y medios como medida de control, en forma rutinaria.
    1. El análisis de cualquier archivo recibido por red o por cualquier forma de medio de almacenamiento, para detectar malware, antes del uso.
    2. El análisis de los archivos adjuntos y descargas enviados por correo electrónico, para la detección de malware antes del uso, este análisis deberá llevarse a cabo en todos los dispositivos de la organización.
- Definir procedimientos y responsabilidades relacionadas a la protección contra el malware en los sistemas, proveer de formación acerca del uso de dichos procedimientos, reporte y recuperación de ataques de malware.
- Preparación de planes de contingencia para la continuidad del negocio apropiados, para la recuperación de ataques,

incluyendo todos los datos necesarios, copias de respaldos y disposiciones de recuperación.

- Implementar procedimientos para recolectar información de forma regular, ejemplo suscripción a sitios web que proporcionen información de nuevos malware, los mismos deberán ser exactos e informativos, usar fuentes calificadas, publicaciones periódicas sitios o proveedores de internet confiables.
- Aislamiento de entornos en donde se pueden obtener impactos catastróficos.

Información adicional

Es necesario la protección contra la introducción de malware en las etapas de mantenimiento y de emergencia.

Bajo condiciones determinadas, la protección contra malware puede causar perturbaciones dentro de las operaciones.

- **Copia de seguridad**

Objetivo: Proteger contra la perdida de datos.

- ✓ **Información de respaldo**

Control

Se debe hacer copias de respaldo de información, de software e imágenes de los sistemas, y poner a prueba regularmente confirme a una política de copias de respaldo aceptada.

Guía de implementación

Se debe establecer una política de respaldos y definir los requisitos de la organización para las copias de respaldos información, software y sistemas.

La política debe definir requisitos de retención y protección.

Proporcionar instalaciones adecuadas para almacenar las copias de respaldo, para asegurar la información y software esenciales para la recuperación después de un desastre o falla del medio.

Tomar en cuenta los siguientes aspectos para el diseño y elaboración de copias de respaldo:

- Se debe producir registros exactos y completos de las copias de respaldo, y los procedimientos de restauración documentados.
- La cobertura (ejemplo: copias de respaldo completas o diferenciales) y la frecuencia con que se hagan las copias de respaldo deben reflejar los requisitos de negocio de la organización, los requisitos de la información involucrada, y la criticidad de la información para la operación continua de la organización.
- Las copias de respaldo se deben almacenar en un lugar remoto, a una distancia suficiente que permita escapar de cualquier daño que pueda ocurrir en el sitio principal.
- Se debe dar un nivel apropiado de protección física y entorno a la información del respaldo.
- Los respaldos se deben poner a prueba regularmente para asegurar que se puede depender de ellos para uso de emergencia en caso de ser necesario, lo cual se debe combinar con las pruebas del procedimiento de restauración, y verificar el tiempo en que se lleva a cabo la restauración requerida, mantener un medio de pruebas donde se los aplicara la restauración.
- En situación en las que la confidencialidad tiene importancia, las copias de respaldo deben estar protegidas por medios de encriptación.

Llevar registro documental de las operaciones realizadas con las copas de respaldo y tener en cuenta las fallas de respaldo programadas.

- ✓ **Realización y frecuencia del respaldo**

Control

Se sugiere tener un mínimo de 3 copias de los respaldos de información la primera en forma local en los dispositivos, la segunda fuera de los dispositivos en medios de almacenamiento y la tercera fuera de la organización (ejemplo nube externa).

Guía de implementación

Tomar en cuenta los siguientes puntos para mantención de los respaldos.

- Para una mejor administración de espacios de almacenamiento se sugiere aplicar una política de almacenamiento de respaldos, la información destinada al archivo o almacenamiento será la información de la empresa correspondiente a la de 10 años atrás del año en curso.

- El plan de almacenamiento de respaldos de información es el siguiente:

  - Los últimos 9 años se almacenará 2 respaldos por año, el respaldo de medio año y de fin de año.
  - El año actual debe almacenar el respaldo de cada fin de mes.
  - El último mes se almacenarán 1 respaldo semanal.
  - La última semana se realizará un respaldo diario.

- **Registro y control**

  Objetivo: registrar eventos y generar evidencias.

  - ✓ **Registro**

    Control

    Se debe registrar, revisar y proteger las actividades de los usuarios periódicamente, excepciones, fallos y eventos de seguridad de información.

    Guía de implementación

    Los registros de eventos relevantes deben incluir:

    - Identificador del usuario (ID)
    - Actividades del sistema
    - Fechas, hora, y detalles de eventos clave ejemplo conexión (log-on) y desconexión (log-off)
    - Identificador de dispositivo y sistema, localización del mismo.
    - Registros de intentos de acceso a los sistemas, y recursos de red, exitosos y fallidos.
    - Registro de cambios de configuración.
    - Uso de privilegios
    - Uso de utilidades y aplicaciones del sistema
    - Direcciones y protocolos de red
    - Alarmas generadas por el control de acceso.
    - Registro de activación y desactivación de los sistemas de protección, ejemplo software de antivirus y detección de intrusión.
    - Registro de transacciones ejecutas por el usuario en las aplicaciones.

El registro de eventos establece las bases para los sistemas automatizados de supervisión que son capaces de generar informes y alertas sobre la seguridad del sistema.

Información adicional

Los registros de eventos pueden contener datos sensibles y personales. Para lo cual tomar medidas adecuadas de protección de datos personales.

En medida de lo posible, los administradores del sistema no deben tener permisos para borrar o desactivar los registros de sus propias actividades.

- ✓ **Registro de administración y operación**

Control

Se debe registrar, revisar y proteger las actividades del o los administradores del sistema y sus operadores.

Guía de implementación

Los usuarios con privilegios elevados pueden ser capaces de manipular los registros en las infraestructuras de tratamiento de información, lo cual hace necesario proteger y revisar los registros para mantener las responsabilidades de los usuarios con privilegios elevados.

Información adicional

Utilizar para la supervisión de las actividades del sistema y el cumplimiento de las actividades de administración de la red y sistemas, un sistema de detección de intrusos administrado fuera del control de los administradores del sistema y de la red.

- ✓ **Sincronización de relojes**

  Control

  Los relojes de toda la infraestructura de tratamiento de información dentro de la organización, deben estar sincronizados con una única fuente de tiempo precisa y acordada.

  Guía de implementación

  Se debe documentar los requisitos externos e internos para la representación, sincronización y precisión del tiempo.

  Debe documentarse e implementarse el enfoque de la organización para obtener un tiempo de referencia de una fuente externa, así como la forma de sincronización de los relojes internos.

  Información adicional

  La correcta configuración de los relojes de los equipos es importante para garantizar la precisión de los registros de auditoría, que pueden requerirse para una investigación o como evidencia en casos legales o disciplinarios.

- ➢ **Control de software operativo.**

  Objetivo: asegurar la integridad del software.

  - ✓ **Instalación de software en sistema operativos**

    Control

    Se debe implementar procedimientos para el control de instalación de software.

    Guía de implementación

    Se debe tener en cuenta las siguientes directrices para el control de instalación de software en sistema operativos:

- Las actualizaciones de los sistemas operativos, aplicaciones y bibliotecas de programas solo deben ser llevada a cabo por administradores formados con la adecuada autorización de la dirección.
- Los sistemas operativos solo deben manejar códigos ejecutables aprobados y no códigos de desarrollo o compiladores.
- Debe emplearse un sistema de control de configuración para supervisar todo el software implantado, así como la documentación del sistema.
- Se deben implementar puntos de restauración antes de cada actualización o instalación.
- Debe mantenerse un registro de auditoría de todas las actualizaciones de las bibliotecas de los programas instalados.
- Debe conservarse versiones anteriores del software de las aplicaciones como medida de contingencia.
- Debe archivarse las versiones antiguas de software, junto con requerimientos, parámetros y procedimientos de instalación, detalles de la configuración y software de apoyo durante el tiempo en que se mantenga el archivo.

Todo software adquirido a proveedores que se utilice en los sistemas operativos debe mantenerse a nivel que cuente con la asistencia técnica del proveedor. La organización debe considerar los riesgos de utilizar software sin contar con asistencia técnica.

Se deben aplicar parches de software cuando sea necesario, para ayudar a reforzar o eliminar los puntos débiles de la seguridad.

Solo debe concederse acceso físico o lógico a los proveedores para que presten servicios de asistencia técnica, solo en los casos necesarios y con la autorización de la dirección. Toda actividad de los proveedores debe supervisarse.

- ✓ **Gestión de vulnerabilidades técnicas.**

  Control

  Se debe obtener información oportuna de todas las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición a dichas vulnerabilidades y adoptar medidas adecuadas para mitigar o afrontar el riesgo asociado.

  Guía de implementación

  La información específica que se requiere para el soporte y gestión de las vulnerabilidades técnicas debe incluir el proveedor de software, versiona miento, estado actual de implantación (ejemplo software aplicación instalada en que sistema) y el usuario o usuarios de la organización que se responsabilice del software.

  Adoptar medidas adecuadas y oportunas como respuesta a la identificación de posibles vulnerabilidades técnicas, seguir las siguientes directrices con el fin se establecer un proceso efectivo en la gestión de vulnerabilidades técnicas:

  - La organización debe definir y estableces funciones y responsabilidades asociadas a la gestión de las vulnerabilidades técnicas, supervisión, evaluación de riesgos, parcheo, seguimiento de activos y cualquier responsabilidad de coordinación necesaria.
  - Debe identificarse los recursos de información que serán usados para la identificación de las vulnerabilidades técnicas y mantener alertas sobre ellas, para software y tecnologías, estos recursos deben actualizarse según se modifique el inventario o cuando se encuentre o cuando se añadan nuevos recursos de utilidad.
  - Definir una escala temporal para reaccionar a notificaciones de vulnerabilidades que sean relevantes.

- Una vez identificadas las vulnerabilidades, la organización debe identificar los riesgos asociados y medidas que se adoptaran, las cueles pueden incluir parches, actualizaciones u otros controles.
- De existir un parche de una fuente legitima, debe evaluarse los riegos de la instalación del mismo y comprarlos con los riesgos de la vulnerabilidad.
- Las actualizaciones y parches deben ser probada y evaluadas antes de su instalación para así garantizar su efectividad y que no tengan efectos secundarios que no puedan ser aceptados. De no existir parches o actualizaciones, considerar los siguientes controles:

    1. Desactivar servicios o capacidades relacionadas con la vulnerabilidad.
    2. Adaptar o incluir controles de acceso, ejemplo, firewall, limitación a nivel de red.
    3. Incremento en supervisión para detectar y evitar ataques reales.
    4. Aumentar la concienciación sobre la vulnerabilidad.

- Mantener un registro de auditoría de todos los procedimientos adoptados.
- Los procesos de gestión de vulnerabilidades deben supervisarse y evaluarse periódicamente para así garantizar su efectividad.
- Sistemas con riesgo elevado deben ser los primeros en tratarse.
- La gestión eficaz de vulnerabilidades debe estar alineado a la gestión de incidentes.
- Definir un procedimiento para considerar la identificación de una vulnerabilidad, pero por la situación de la misma no es posible adoptar una contramedida, la organización debe

evaluar los riesgos relativos de la vulnerabilidad y definir acciones de detección – corrección adecuadas.

- ✓ **Restricción de la instalación**

  Control

  Establecer y aplicar reglas que rijan la instalación de software por parte del usuario.

  Guía de implementación

  La organización debe definir y hacer cumplir una estricta política sobre qué tipo de software puede ser instalados por los usuarios.

  - Aplicar el principio de menor privilegio.
  - Los usuarios deben tener la capacidad de instalar software si se les concede ciertos privilegios.
  - Debe identificarse los tipos de instalación de software permitidas (por ejemplo, actualizaciones y parches de seguridad para el software existente)
  - Definir que instalaciones están prohibidas ejemplo software de uso personal y software de dudosa procedencia o que sea potencialmente maliciosa

  Información adicional

  La instalación sin control de software en equipos informáticos puede llevar a introducir vulnerabilidades cuyas consecuencias pueden ser: fuga de información, perdida de integridad, otros incidentes de seguridad y violación de derechos de propiedad intelectual.

- ➢ **Consideración sobre la auditoria de los sistemas de información**

  Objetivo: minimizar el impacto de actividades de auditoria en sistemas operativos.

- ✓ **Protección de los sistemas de información durante la auditoria**

  Control

  Las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deben ser planificados y acordados cuidadosamente para minimizar el riesgo de interrupciones en los procesos de la organización.

  Guía de implementación

  Se debe cumplir las siguientes directrices:

  - Los requisitos de acceso a sistemas y datos de auditoria deben acordarse con la dirección.
  - Debe controlarse y acordarse el alcance de las comprobaciones durante la auditoria.
  - Deben limitarse las comprobaciones a acceso de solo lectura al software y a los datos.
  - Aquellas pruebas de auditoría que puedan afectar la disponibilidad del sistema deben ejecutarse fuera del horario laboral
  - Todos los accesos deben ser supervisados y registrados para obtener una pista de referencia.

- ➢ **Gestión de la seguridad de red**

  Objetivo: asegurar y mantener la protección de la información en las redes y recursos de tratamiento de información.

  - ✓ **Seguridad en las redes**

    Control

    Las redes deben ser gestionada y controladas para protección de la información en los sistemas y aplicaciones.

Guía de implementación

Deben ser implementados los controles para garantizar la seguridad de la información en las redes y la protección de servicios conectados frente a accesos no autorizados, considerar los siguientes puntos:

- Debe establecerse las responsabilidades y procedimientos para la gestión de los equipos de red.
- La responsabilidad operacional de redes debe estar separada de las operaciones de sistemas informáticos, donde sea apropiado.
- Debe establecerse controles para salvaguardar la confidencialidad e integridad de los datos que pasa por la red sea pública o redes inalámbricas, proteger los sistemas conectados y sus aplicaciones.
- Debe realizarse un registro adecuado de eventos y monitorización que permita la detección de acciones que podrían afectar, ser relevantes, para la seguridad de la información.
- Toda actividad de gestión debe estar estrechamente coordinada, tanto para la optimización de los servicios, como para asegurar controles y su aplicación conscientemente en la toda la infraestructura de tratamiento de la información.
- Todo sistema de red debe ser autenticado
- Debe ser restringida las conexiones a los sistemas a la red

✓ **Seguridad en los servicios de red**

Control

Se debe identificar mecanismos de seguridad, niveles de servicio, y los requisitos de gestión en todos los servicios de red, se debe incluir cualquier acuerdo de servicio de red, tanto para servicios dentro de la organización como los que se subcontratan.

Guía de implementación

Se determinará y supervisará la capacidad del proveedor del servicio de red para la gestión de los servicios acordados de manera segura, de igual manera se acordará el derecho a ser auditado.

Se debe asegurar e identificar que los proveedores de servicios de red implanten medidas de características de seguridad, niveles de servicio y requisitos de gestión.

Información adicional

Los servicios de red incluyen la provisión de conexiones, servicios de red privada, soluciones de seguridad de red gestionada, como, firewalls, detección de intrusiones.

Algunas características de seguridad de los servicios de red podrían ser:

1. Tecnología aplicada a la seguridad de red, como, autenticación, cifrado y controles de conexión.
2. Parámetros técnicos requeridos para la conexión, reglas de seguridad y conexión a las redes.
3. Procedimientos para restricción de los servicios de red donde sea necesario.

- ✓ **Segregación de redes**

Control

Deben estar segregados en redes distintas, los grupos de servicios de información, los usuarios y los sistemas de información.

Guía de implementación

Un método para gestionar la seguridad de grandes redes se basa en dividirlas en dominios de red separados. Los dominios se eligen según niveles de confianza o unidades organizativas, o una

combinación de ambos. La segregación se puede hacer usando redes físicas o lógicas diferentes.

El perímetro de cada dominio de red y controlar el acceso entre ellos usando una pasarela (ejemplo: firewall, router filtrado). El criterio para la segregación y el acceso se basa en la evaluación de los requisitos de seguridad de cada dominio, la política de control de acceso, el valor y la clasificación de la información, y el coste y el impacto de la pasarela.

Las redes inalámbricas y cómo se deberían considerar como conexiones externas y segregarlas de las redes internas. Definir el criterio para la segregación y el acceso basado en la evaluación de los requisitos de seguridad, la política de controles de red y otros factores.

Información adicional

Habitualmente, las redes se extienden más allá de los límites de la organización debido a la creación de negocios colaborativos con otras empresas que requieren la interconexión o compartición de los recursos de red para el tratamiento de información. Estas pueden aumentar el riesgo de acceso no autorizado de los sistemas de información de la organización que usa la red, alguno de los cuales requerirá protección de otros usuarios de la red debido a su sensibilidad o criticidad.

- **Intercambios de información**

Objetivo: Mantener la seguridad de la información que se intercambia o transfiere dentro de la organización o con cualquier entidad externa.

- ✓ **Transferencia de información**

  Control

  Deben establecerse procedimientos y controles formales para la protección en el intercambio de información mediante el uso de cualquier tipo de recursos de comunicación.

  Guía de implementación

  Tomar en consideración los siguientes aspectos para los procedimientos y controles a seguirse para el uso de recursos de comunicación:

  - El diseño del procedimiento debe proteger la información transferida de: interceptación, copia, modificación, errores de enrutamiento y destrucción.
  - Procedimiento para la detección en contra de malware que podría ser enviado o receptado a través del uso de comunicaciones electrónicas.
  - Procedimientos para proteger información electrónica sensibles en forma de adjuntos.
  - Responsabilidades del personal, partes externas, y de cualquier otro usuario de no comprometer a la organización, ejemplo, difamación, acoso, suplantación, reenvió de mensajes en cadena o spam, las compras no autorizadas, etc.
  - Uso de técnicas criptográficas, ejemplo para la protección de la confidencialidad, integridad y autenticidad de la información.
  - Directrices establecidas por la organización para retención, eliminación de toda correspondencia comercial e inclusión de mensajes.
  - Controles y restricciones asociados al uso de los recursos de comunicación, ejemplo: reenvió automático de correos electrónicos a direcciones de correo externas.

- Capacitar y asesorar al personal que tenga las precauciones necesarias de no revelar información confidencial.
- Tener la precaución de no dejar mensajes que contenga información confidencial en los contestadores automáticos, porque podrían ser reproducidos por personas no autorizadas, almacenados en sistemas públicos o de manera incorrecta como consecuencia de un error.
- Recordar al personal que no debe tener conversaciones confidenciales en lugares públicos o haciendo uso de canales de comunicación inseguros, oficinas abiertas, lugares de reunión.

Información adicional

La transferencia de información puede ser realizada mediante un conjunto de diferentes tipos de recursos de comunicación, incluyendo, dispositivos de almacenamiento, correo electrónico, voz y video.

- ✓ **Acuerdos de confidencialidad y no divulgación**

Control

Deben identificarse, establecerse, documentarse y revisarse regularmente los acuerdos de confidencialidad y no divulgación.

Guía de implementación

Los acuerdos de confidencialidad o de no revelación son contratos que protegen la información privada de ser divulgada a terceros no autorizados. Estos acuerdos se pueden aplicar tanto a entidades externas como a empleados de la organización. Los elementos que deben incluirse en estos acuerdos dependen del tipo de la otra parte y del uso que se le dará a la información confidencial. Algunos elementos que se deben considerar son:

- Se debe definir la información a proteger, ejemplo información confidencial.
- Definir la duración prevista para el acuerdo, incluyendo los casos en que la confidencialidad tenga la necesidad de mantener indefinidamente.
- Definir las acciones necesarias cuando los acuerdos se terminen.
- Responsabilidades y acciones de los firmantes para evitar la revelación no autorizada de la información.
- Definir la propiedad de la información, los secretos comerciales y propiedad intelectual, y su relación con la protección de información confidencial.
- Se debe delimitar el uso permitido de la información confidencial y los derechos del firmante y el uso que le dará a la información.
- Establecer el derecho a auditar y supervisar las actividades que involucres la información confidencial.
- Mantener procesos para notificar y avisar la revelación no autorizada o fugas de información confidencial.
- Contemplar los términos en que la información deba ser devuelta o destruida en el cese de los acuerdos.
- Estableces acciones que sean tomadas en caso de incumplimiento del acuerdo.

Los acuerdos de confidencialidad y no divulgación deben cumplir con toda la ley y reglamentos aplicables en la jurisdicción a la que corresponda.

Información adicional

Los acuerdos de confidencialidad y no divulgación protegen la información de la organización e informan las responsabilidades de los firmantes relacionados a la protección, utilización y revelación de información de forma responsable y autorizada.

Las organizaciones necesitaran utilizar diferentes tipos de acuerdos de confidencialidad y no divulgación en diferentes circunstancias.

- **Seguridad en los procesos de desarrollo y apoyo**

  Objetivo: garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de los sistemas de informa.

  - ✓ **Ciclo de vida de desarrollo seguro**

    Control

    Se debe establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas seguros.

    Guía de implementación

    El desarrollo seguro es un requisito indispensable para el desarrollo de un servicio, arquitectura, software y sistemas seguros. Como tal dentro de la policía de desarrollo seguro, se debe considerar los siguientes aspectos:

    - Seguridad en el entorno de desarrollo
    - Directrices en la seguridad del ciclo de vida de desarrollo de software:
      1. Seguridad en la metodología de desarrollo
      2. Guías de desarrollo seguro para cada lenguaje de programación.
    - Requisitos de seguridad en la fase de diseño
    - Puntos de verificación de seguridad enlazados en cada hito del proyecto.
    - Repositorios seguros
    - Seguridad en el control de versiones
    - Conocimiento necesario sobre seguridad de aplicaciones
    - Capacidad en los desarrolladores para evitar, encontrar y reparar vulnerabilidades

Se recomienda utilizar técnicas de programación segura tanto en nuevos desarrollos como en la reutilización de código, especialmente cuando las normas aplicadas en el desarrollo original pueden no ser conocidas o no estar actualizadas con las mejores prácticas actuales. Es importante tener en cuenta las normas de programación segura y seguir las indicaciones correspondientes. Los desarrolladores deben recibir formación en el uso de estas técnicas y las pruebas y revisiones de código deben asegurar que se han aplicado correctamente.

La organización debe asegurarse de que la parte externa cumpla con estas normas de desarrollo seguro en el caso de subcontratar el desarrollo.

- ✓ **Gestión de cambios**

  Control

  Los usos de procedimientos formales de control de cambios deben implementarse durante todo el ciclo de vida del desarrollo.

  Guía de implementación

  Es importante documentar y hacer cumplir los procedimientos formales de control de cambios tanto en las etapas iniciales del diseño como en el mantenimiento posterior. Esto garantiza la integridad del sistema, las aplicaciones y los productos.

  Al incorporar nuevos sistemas y realizar cambios importantes en los sistemas existentes, se debe seguir un proceso formal que incluya documentación, especificaciones, pruebas, control de calidad y gestión de la implementación.

  Este proceso también debería asegurarse de que los procedimientos de seguridad y de control existentes no se vean comprometidos, que a los programadores de apoyo se les habilite el acceso sólo a

aquellas partes del sistema necesarias para su trabajo y que se obtiene el acuerdo formal y la aprobación de cualquier cambio.

- Mantener un registro de los niveles de autorización aprobados
- Asegurar que los cambios enviados sean a los usuarios autorizados.
- Revisión de controles y procedimientos de desarrollo integro para asegurar que no se vean comprometidos por los cambios.
- Mantener identificado software, información, entidades de bases de datos, hardware que requiere cambios.
- Identificar y comprobar la seguridad de código crítico para minimizar la probabilidad de fallos de seguridad.
- Aprobación anticipada de propuestas antes de iniciar los cambios.
- Aceptación de los cambios por parte de usuarios autorizados antes de la colocación en producción.
- Adaptación de documentación operativo y procedimientos de usuario, en el caso de ser necesario.
- Implementación de cambios en los momentos adecuados para que no interrumpa en los procesos de la organización.

Información adicional

Las buenas prácticas incluyen pruebas del nuevo software, pero siempre en un entorno segregado de los entornos de explotación y desarrollo, esto permite la protección adicional de la información operacional que se usa en pruebas, esto debe aplicarse a parches, *service pack*, y todo tipo de actualizaciones.

- ✓ **Arquitectura de sistemas seguros y principios de ingeniería**

  Control

Se debe establecer, documentar, mantener y aplicar todos los esfuerzos de implementación de sistemas de información.

Guía de implementación

Es importante establecer y documentar procedimientos de ingeniería de sistemas de información seguros, siguiendo los principios de ingeniería de seguridad. Estos procedimientos deben aplicarse a las actividades internas de ingeniería de sistemas de información.

La seguridad debe ser considerada en todas las capas de la arquitectura, incluyendo las de negocio, datos, aplicaciones y tecnología. Es necesario equilibrar la necesidad de seguridad de la información con la necesidad de accesibilidad. Además, se deben analizar los riesgos de seguridad de las nuevas tecnologías y revisar el diseño en busca de posibles patrones de ataque conocidos.

Los principios y procedimientos de ingeniería establecidos deben revisarse periódicamente para asegurar que estén contribuyendo de manera efectiva a la mejora de normas de seguridad en los procesos de ingeniería.

Los principios de ingeniería de seguridad deben aplicarse a los sistemas de información externos a través de contratos y acuerdos vinculantes entre la organización y sus proveedores contratados. La organización debe asegurarse de que los proveedores cumplen con los mismos estándares de ingeniería de seguridad que ellos. Es importante confirmar que los proveedores mantienen un nivel de rigor comparable en términos de seguridad.

Información adicional

Los procedimientos de desarrollo de aplicaciones deben incorporar técnicas de ingeniería de seguridad en aquellas aplicaciones que tienen interfaces de entrada y salida. Estas técnicas ofrecen

orientación sobre aspectos como la autenticación de usuarios, el control de sesiones seguras, la validación y depuración de datos, y la eliminación de códigos de depuración. Al aplicar estas técnicas, se fortalece la seguridad de las aplicaciones y se reducen los riesgos asociados con posibles vulnerabilidades.

- ✓ **Separación de entornos de desarrollo, pruebas y producción**

  Control

  La organización debe establecer y proteger de manera adecuada los entornos de desarrollo seguro e integrar todos los esfuerzos que rigen sobre todo el ciclo de vida del desarrollo del sistema.

  Guía de implementación

  El entorno de desarrollo seguro incluye los usuarios, procesos, tecnologías relacionadas con el desarrollo e integración de sistemas.

  La organización debe tener en cuenta los siguientes puntos:

  - La sensibilidad de los datos a ser procesados, almacenados y transmitidos por el sistema.
  - Requisitos externos e internos aplicables, ejemplos reglamentos y políticas.
  - Los controles de seguridad implementados por la organización que apoyen al desarrollo del sistema.
  - Honradez del personal al trabajar en el entorno.
  - Controles de acceso al entorno de desarrollo.
  - Monitorizar los cambios en el entorno y el código almacenado en el mismo.
  - Almacenamiento seguro de las copias de respaldo fuera de las instalaciones.
  - Mantener el control del movimiento de los datos desde y hacia el entorno.

Una vez determinado los niveles de protección para un entorno de desarrollo seguro, la organización debe documentar el proceso en los procedimientos de desarrollo seguro y dar a conocer a todos los usuarios que lo necesiten.

- ✓ **Desarrollo externalizado**

  Control

  El desarrollo de software externo debe ser supervisado o controlado por la organización.

  Guía de implementación

  Se debe considerar los siguientes puntos:

  - Los acuerdos de licencias, propiedad del código, derechos de la propiedad intelectual relacionados con los contenidos subcontratados.
  - Requisitos contractuales para las prácticas de diseño seguro, codificación y pruebas.
  - Pruebas de aceptación de calidad y adecuación de entregas.
  - Presentación de pruebas de que se usan umbrales de seguridad para establecer los niveles mínimos aceptables de seguridad y calidad.
  - Presentación de bitácora de pruebas para protección de contenido malicioso, intencionado como no intencionado, igual para la protección contra vulnerabilidades conocidas.
  - Derecho contractual para auditar procesos y controles de desarrollo
  - Documentación real para el entorno de complicación utilizado para crear reportes entregables.

- ✓ **Pruebas de seguridad en el desarrollo y la aceptación**

  Control

Se debe llevar a cabo pruebas de la seguridad funcional y establecer un plan de pruebas de aceptación y criterios relacionados para los nuevos sistemas de información, actualizaciones y nuevas versiones.

Guía de implementación

Los sistemas nuevos y los actualizados requieren pruebas y verificación exhaustivas en los procesos de desarrollo, incluyendo la preparación de un plan detallado de actividades y datos de prueba junto a los resultados esperados bajo las condiciones establecidas.

Para los desarrollos propios, se recomienda que el equipo de desarrollo realice pruebas iniciales. Además, se deben llevar a cabo pruebas de aceptación independientes tanto en desarrollos internos como en desarrollos externalizados para garantizar que el sistema funcione según lo esperado.

Las pruebas de aceptación del sistema deberían incluir los requisitos de seguridad de la información y de que se han aplicado las prácticas de desarrollo seguro del sistema.

Las pruebas también deberían llevarse a cabo sobre los componentes recibidos y los sistemas integrados. La organización puede utilizar herramientas automatizadas, como las herramientas de análisis de código o los escáneres de vulnerabilidad, y verificar la solución de los defectos relacionados con la seguridad.

Es recomendable llevar a cabo las pruebas en un entorno de prueba que simule de manera realista el entorno de la organización. Esto garantiza que el sistema no introducirá vulnerabilidades y que las pruebas realizadas son confiables.

- **Gestión de incidentes y continuidad de la seguridad de la información**

  Objetivo: Asegurar un guía coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.

  - ✓ **Planificación y preparación de la gestión de incidentes de seguridad**

    Control

    Se debe establecer un plan y procedimientos de gestión que garanticen una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.

    Guía de implementación

    Tomar en consideración las siguientes directrices en los procedimientos que gestiones los incidentes de seguridad:

    - Se debe planificar la gestión de los siguientes procedimientos para una comunicación adecuada dentro de la organización:

      1. Procedimientos de plan y preparación de respuesta a incidentes.
      2. Procedimientos de monitoreo, detección, análisis, y comunicación de eventos e incidentes de seguridad.
      3. Procedimientos para registrar las actividades de gestión de incidentes
      4. Procedimientos de manejo de pruebas forenses.
      5. Procedimientos para la evaluación y toma de decisiones sobre eventos de seguridad.
      6. Procedimientos de respuesta que incluyen referentes al escalado, la recuperación de manera controlada frente a un incidente, comunicación a personas internas y externas o a terceras organizaciones.

- Considerar procedimientos que aseguren que:

1. Personal capacitado que maneje los asuntos relacionados a incidentes de seguridad de la información al interior de la organización.
2. Implantar un punto de contacto para la detección y comunicación de eventos e incidentes.
3. Mantener contactos apropiados con las autoridades, grupos de interés externos al que con foros que traten asuntos relacionados a eventos e incidentes.

- Deben incluirse en los procedimientos de comunicación:

1. Preparar formularios de notificación de seguridad de la información para respaldar el proceso de notificación y ayudar al denunciante a recordar toda la información necesaria en caso de un incidente de seguridad de la información
2. Acciones apropiadas a tomar en caso de un incidente de seguridad de la información; por ejemplo, anote de inmediato todas las cosas importantes (como el tipo de delito, el error, los mensajes en la pantalla...), notifique a la persona de inmediato y tome medidas formales
3. Describir al proceso disciplinario establecido para tratar con empleados, contratistas u otras personas que violen la seguridad.
4. El proceso de retroalimentación es suficiente para asegurar que aquellos que reportan incidentes de protección de datos estén informados del resultado una vez que el problema ha sido resuelto y cerrado.

- ✓ **Informe de eventos de seguridad de la información**

  Control

  Todo evento de seguridad de la información debe informarse de manera inmediata por canales adecuados.

  Guía de implementación

  Todos los empleados, contratistas y terceros deben ser conscientes de su obligación de comunicar cualquier incidente de seguridad de datos a la mayor brevedad. También deben saber cómo reportar incidentes de protección de datos y con quién puedes contactar.

  Las siguientes situaciones se consideran para informar eventos de seguridad:

  - Control eficaz de la seguridad.
  - Incumplimiento a los pilares de la información: integridad, confidencialidad y disponibilidad
  - Errores de los usuarios
  - Incumplimiento a políticas o directrices.
  - Infracciones a las directrices de seguridad física.
  - Cambios sin control en los sistemas.
  - Anomalías en software o hardware.
  - Velaciones de acceso.

  Información adicional

  Los errores u otro comportamiento inusual del sistema pueden ser una indicación de un ataque o una violación de la seguridad y siempre deben informarse como un incidente de seguridad de la información.

- ✓ **Evaluación y decisión sobre los eventos**

  Control

  Cada uno de los eventos de seguridad de la información debe ser evaluado y debe decidirse si se clasifica como incidente.

  Guía de implementación

  El responsable como punto de contacto debe evaluar cada incidente de seguridad de la información utilizando los criterios establecidos de incidente de seguridad y nivel de incidente y decidir si debe clasificarse como un incidente.

  La planificación de eventos y la priorización de eventos pueden ayudar a identificar las tendencias y el crecimiento de los eventos.

  En los casos en que la organización tenga un Equipo de respuesta de seguridad de la información (Information Security Incident Response Team, ISIRT), los objetivos y las decisiones pueden remitirse al equipo para su confirmación o revisión.

  Los resultados de las pruebas y las conclusiones deben documentarse en detalle para futuras referencias y análisis.

- ✓ **Respuesta a los incidentes de seguridad de la información**

  Control

  Los incidentes de seguridad deben ser respondidos conforme a los procedimientos documentados.

  Guía de implementación.

  Todo incidente de seguridad de información debe ser comunicado al responsable como punto de contacto, como a otras personas relevantes de la organización o terceras partes:

La respuesta a incidentes debe incluir los siguientes procedimientos:

- Recopilación de evidencia inmediatamente después de la ocurrencia del incidente.
- La realización de un análisis forense de seguridad de la información en los casos requeridos.
- Escalado del incidente, en los casos que se requiera.
- Asegurar que todas las personas involucradas en las actividades de respuesta a incidentes participen plenamente en la realización de evaluaciones de seguimiento
- Solo notificar la existencia de un evento de seguridad de datos o cualquier otra información relevante a todas las partes internas y externas o terceros que necesiten saber.
- Gestionar las debilidades de seguridad de la información que pueden causar o contribuir al incidente
- después de la resolución satisfactoria del incidente, el cierre formal y registro del evento.

Después del análisis del incidente, se debe identificar la fuente del incidente, si es necesario.

Información adicional

El objetivo principal de la respuesta a incidentes es restaurar la "seguridad a la normalidad" y comenzar la recuperación correctamente.

- ✓ **Aprender de los incidentes de seguridad de la información**

Control

La información obtenida del análisis y corrección de incidentes de seguridad de la información debe utilizarse para reducir la probabilidad o el impacto de futuros incidentes.

Guía de implementación

Deben existir métodos para medir, rastrear y monitorear la calidad, el volumen y el costo de las operaciones de seguridad de la información.

La información obtenida del análisis de incidentes de seguridad de la información debe utilizarse para identificar incidentes comunes o críticos.

Información adicional

Un análisis de eventos de seguridad de la información puede indicar la necesidad de mejorar o aumentar los controles para reducir la frecuencia, el daño y el costo de eventos futuros, o para centrarse en ellos en el análisis.

Debido a problemas de privacidad, los incidentes de seguridad de la información se pueden utilizar en estudios de concienciación del usuario como ejemplos de lo que puede suceder, cómo responder a dichos incidentes y cómo protegerse en el futuro.

- ✓ **Recogida de pruebas**

  Control

  La organización debe definir e implementar procedimientos para la búsqueda, recolección, obtención y almacenamiento de información que pueda servir como evidencia.

Guía de implementación

Se deben desarrollar procedimientos internos que se seguirán en la recopilación y presentación de pruebas con el propósito de enjuiciamiento penal.

En general, estos métodos de recopilación de evidencia deben incluir métodos de detección, recopilación, captura y almacenamiento de evidencia basados en diferentes tipos de medios, dispositivos y sus estados (por ejemplo, si están encendidos o apagados). Puntos a considerar:

- La cadena de custodia
- Integridad de la evidencia
- Protección de las personas
- Funciones o responsabilidades de los usuarios implicados
- Competencia del personal
- Documentación y resumen.

De ser posible, se deben proporcionar certificados u otros métodos adecuados para verificar las credenciales de los trabajadores y el equipo utilizado, a fin de agregar valor a la evidencia conservada.

La prueba futura puede cruzar los límites organizativos o administrativos. En estos casos, se debe asegurar que la organización tiene la capacidad de recolectar la información necesaria como prueba. Las necesidades de otras áreas también deben tenerse en cuenta para aumentar las posibilidades de ser aceptado en todas las áreas relevantes.

Información adicional

La información es el proceso de encontrar, identificar y documentar evidencia potencial. Coleccionar es el proceso de encontrar activos que puedan tener potencial.

La copia es el proceso de hacer una copia física de los datos. La preservación es el proceso de preservar y preservar la integridad original y el nivel de evidencia potencial.

Cuando se detecta por primera vez un incidente de protección de datos, es posible que no esté claro si el incidente conducirá a una acción legal.

Debido a esto, existe el riesgo de que las pruebas necesarias se destruyan de forma intencionada o accidental antes de que suceda lo peor. Se recomienda utilizar los servicios de un abogado o de la policía al comienzo de cualquier caso pendiente en los tribunales, así como buscar asesoramiento sobre las pruebas necesarias.

- ✓ **Seguridad de la información durante la interrupción**

Control

La organización debe determinar las necesidades de seguridad de la información y la continuidad de la seguridad de la información en situaciones adversas, como durante una crisis o un desastre.

Guía de implementación

La organización debe asegurarse de que el procesamiento de la información se refiera a operaciones de continuidad del negocio o recuperación ante desastres. La seguridad de la información debe tenerse en cuenta al planificar la continuidad del negocio y la recuperación ante desastres.

En ausencia de planes de continuidad del negocio y recuperación ante desastres, la gestión de la seguridad de la información debe

asumir que la seguridad de la información es la misma tanto en circunstancias adversas como normales.

Además, la organización puede realizar una auditoría de seguridad de la información comercial para determinar los requisitos de seguridad de la información que se aplican en el peor de los casos.

Información adicional

Para reducir el tiempo y el esfuerzo dedicados al análisis comercial "extendido" del proceso de seguridad de la información, se recomienda que estos detalles se procesen en el proceso de análisis comercial que se lleva a cabo durante el proceso administrativo o la respuesta comercial ante desastres.

Esto significa que el conocimiento de las necesidades de desarrollo está claramente definido en la gestión de procesos de negocio o proceso de recuperación de riesgos.

- ✓ **Preparación de las TIC para la continuidad de la actividad**

Control

La organización desarrollará, escribirá, implementará y mantendrá procesos, procedimientos y sistemas para garantizar el nivel requerido de desempeño de seguridad de la información en situaciones adversas.

Guía de implementación

Una organización debe asegurar que:

- Debe existir un sistema de gestión adecuado para reducir las consecuencias y responder al evento perturbador utilizando personal con la autoridad, conocimientos y habilidades necesarios.

- El personal de respuesta a incidentes está designado y tiene las responsabilidades, facultades y capacidades necesarias para manejar el incidente y garantizar la seguridad de la información.
- Se crean y adoptan planes y procedimientos escritos para la respuesta y la recuperación, que describen cómo la organización gestionará el evento de riesgo y protegerá la seguridad de su información en una situación determinada de acuerdo con los planes operativos de seguridad de la seguridad de la información aceptada.

De acuerdo con los requisitos de información continua, la organización crea, registra, utiliza herramientas y mantiene:

- Gestión de la seguridad de la información en sistemas, procesos y aplicaciones, así como herramientas para apoyar la continuidad del negocio o la recuperación ante desastres.
- Mantener métodos, procedimientos y cambios operativos para proteger la seguridad de la información durante una crisis
- Permitir controles compensatorios para aquellos controles de seguridad de la información que no puedan mantenerse durante una situación adversa.

Información adicional

Se pueden definir procesos y procedimientos específicos para fines de continuidad del negocio o recuperación ante desastres. La información gestionada con su ayuda o con la ayuda de sistemas de información especiales debe ser protegida.

Por lo tanto, la organización debe contratar expertos en seguridad de la información para desarrollar, implementar y mantener

operaciones comerciales o sistemas y procesos de recuperación ante desastres.

La aplicación de controles de seguridad de la información debe permanecer vigente durante un evento adverso. Si los controles de seguridad no pueden proteger la seguridad de la información, se deben establecer e implementar otras medidas de seguridad para mantener un nivel aceptable de seguridad de la información.

- ✓ **Preparación de las TIC para la continuidad de la actividad**

Control

La organización debe evaluar regularmente los sistemas que se instalan e implementan para garantizar que sean efectivos y funcionen en condiciones adversas.

Guía de implementación

Los cambios organizativos, tecnológicos, operativos y técnicos, ya sean internos o continuos, pueden dar lugar a cambios en los requisitos de seguridad de la información. En estos casos, las prácticas, los procedimientos y los sistemas de seguridad de la información en curso deben revisarse adecuadamente.

Las organizaciones deben verificar su gestión de la continuidad de la seguridad de la información:

- Implementar y probar sistemas, procesos y herramientas de gestión de la seguridad de la información para garantizar que sean coherentes con los objetivos de seguridad de la seguridad de la información.
- Implementar y evaluar sistemas de información y control para operaciones, procesos y controles de seguridad de la información para garantizar que su implementación sea consistente con los objetivos de seguridad de la seguridad de la información.

- Evaluación de la validez y eficacia de las medidas para garantizar la continuidad de la seguridad de la información al cambiar los sistemas de información, los procesos, los procedimientos y la seguridad de la información o la gestión de procesos comerciales y los métodos de recuperación y resolución si fallan.

Información adicional

Las pruebas de seguridad de los procesos comerciales son diferentes de las pruebas estándar y las pruebas de seguridad de la información y deben realizarse por separado de las pruebas de cambios. Si es posible, es mejor combinar la revisión del control de seguridad de la información con pruebas de desarrollo de negocios o recuperación de riesgos.

- **Cumplimiento de los requisitos legales y contractuales**

Objetivo: Evitar infringir obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información o los requisitos de protección de datos.

- ✓ **Requisitos legales, reglamentarios y contractuales**

Control

Todos los requisitos, ya sean legales, reglamentarios o contractuales, y los procedimientos de la organización para cumplirlos, deben estar claramente definidos, documentados y actualizados en el sistema de información de cada organización.

Guía de implementación

Los controles necesarios y las tareas individuales para cumplir con estos requisitos también deben definirse y documentarse.

Los gerentes o directores deben decidir todas las reglas que aplican a sus organizaciones para satisfacer las necesidades de su tipo de negocio. Si la organización hace negocios en otros países, los

gerentes o directores deben considerar el cumplimiento en todos los países relevantes.

- ✓ **Derechos de propiedad intelectual**

  Control

  Deben implementarse las medidas adecuadas para garantizar el cumplimiento de la ley, los reglamentos y los acuerdos necesarios con respecto al uso de material sobre el que puedan existir derechos de propiedad intelectual, así como el respeto al uso de productos de software.

  Guía de implementación

  Para proteger todo lo que pueda considerarse propiedad intelectual, se deben observar las siguientes reglas:

  - Publicar la ley de propiedad intelectual que define el uso legal de productos de software y productos de información.
  - Solo compre software de fuentes acreditadas y confiables para evitar la infracción de derechos de autor.
  - Mantener información sobre la ley de derechos de propiedad y notificar la intención de tomar medidas disciplinarias contra cualquier empleado que viole esta ley.
  - mantener registros de propiedad e identificar todo activo que requiera protección de derechos de propiedad.
  - Conservar constancia y evidencia de propiedad de licencias, discos maestros, registros, etc.
  - Utilizar controles para garantizar que no se supere el número de usuarios autorizados.
  - Verifique que solo estén instalados el software autorizado y los productos con licencia.
  - Tener una política para cumplir con los términos de las licencias.

- Disponer de una política para la eliminación de software o para transferirlo a un tercero cuando cese su uso.
- No duplicar, ni convierta a otro formato y no elimine nada de una grabación comercial (cine, audio), excepto lo permitido por la ley de derechos de autor.
- No copie libros, artículos, informes u otros documentos, en su totalidad o en parte, a menos que lo permita la ley de derechos de autor.

Información adicional

Los derechos de propiedad intelectual incluyen derechos de software o documentos, diseños, marcas registradas, derechos de autor y licencias de códigos.

Los productos de software genéricos a menudo vienen con un acuerdo de licencia que especifica los términos de la licencia, como limitar el uso del producto a otros dispositivos o limitar las copias solo a copias de seguridad. Los empleados deben ser conscientes de la importancia de los derechos de propiedad intelectual en el software desarrollado por la organización e informarles sobre este tema.

Los requisitos legales, reglamentarios y contractuales pueden imponer restricciones a la copia de material. En particular, pueden exigir que solo se utilicen equipos fabricados, autorizados o disponibles por el fabricante. Las violaciones de los derechos de autor pueden dar lugar a acciones legales, incluidas multas y enjuiciamiento.

- ✓ **Privacidad y protección de la información personal**

Control

La protección de datos y la confidencialidad deben garantizarse de acuerdo con las leyes y reglamentos aplicables.

Guía de implementación

Se debe desarrollar e implementar una política sobre la privacidad y seguridad de la información personal. Esta política debe ser presentada a todas las personas involucradas en el tratamiento de datos personales.

El cumplimiento de esta ley y de las leyes y reglamentos aplicables en materia de privacidad personal y de protección de sus datos requiere de una estructura adecuada para su gestión y control.

A menudo, la mejor manera es nombrar a un oficial de protección de datos que debe orientar a los gerentes, administradores, usuarios y proveedores de servicios sobre sus deberes y procedimientos a seguir.

La responsabilidad de manejar la información personal y garantizar que las políticas de privacidad aceptables cumplan con las leyes y regulaciones aplicables. Se deben tomar las medidas técnicas y organizativas apropiadas para proteger la información personal.

- **Revisiones de la seguridad de la información**

Objetivo: Asegurar que la seguridad de la información se implemente de acuerdo con las políticas y procedimientos de la organización.

- ✓ **Revisión independiente de la seguridad de la información**

Control

El enfoque de la organización para gestionar la seguridad de la información y su uso, es decir, los planes de gestión, los controles, las políticas, los procedimientos y las medidas de seguridad de la información, deben revisarse de forma independiente en tiempos programados o cuando se producen cambios importantes en las operaciones de seguridad.

Guía de implementación

Los administradores deben ordenar una auditoría independiente.

Dicha revisión es necesaria para garantizar la operación y el desempeño continuos de las operaciones de seguridad de la información de la organización.

La evaluación debe incluir una evaluación de las oportunidades de mejora y la necesidad de cambios en el proceso establecido, incluidas las políticas y los planes de gestión.

Esta revisión debe ser realizada por personas independientes del área que se está revisando, como una auditoría interna, un director independiente o alguien contratado por una organización fuera del país para realizar esta revisión. Los desarrolladores deben tener los conocimientos y la experiencia necesarios.

Los resultados de la auditoría independiente deben documentarse y proporcionarse a la dirección que encargó la auditoría. Estos registros deben mantenerse.

Si la evaluación independiente muestra que la seguridad de la información y la implantación no son suficientes, por ejemplo, si los objetivos y requisitos enumerados no se cumplen o no son compatibles con la seguridad de la información en las normas de seguridad de la información, los gerentes deben considerar haciendo cambios.

- ✓ **Cumplimiento de las políticas y normas de seguridad**

Control

Los gerentes deben asegurarse de que todos los procedimientos de seguridad en su lugar de trabajo se implementen correctamente para cumplir con las leyes y estándares de seguridad y cualquier requisito de seguridad aplicable.

Guía de implementación

Los supervisores deben asegurarse de que todas las medidas de seguridad en su lugar de trabajo se utilicen correctamente de acuerdo con las leyes y normas de seguridad y los requisitos de seguridad aplicables.

De existir algún incumplimiento como resultado de la auditoría, los directores o gerentes deberán:

- Identificar las causas del incumplimiento
- Revisar los procedimientos necesarios para el cumplimiento.
- Implementar las acciones correctivas necesarias
- Revisar las medidas correctivas tomadas para probar su eficacia e identificar cualquier error o debilidad.

Los resultados de la inspección y las acciones correctivas tomadas por la gerencia deben registrarse y mantenerse en los registros. Los gerentes o supervisores deben informar los resultados a los auditores independientes cuando se realiza una auditoría en su lugar de trabajo.

- ✓ **Revisión de la conformidad técnica.**

Control

Los sistemas de información deben revisarse periódicamente para verificar que cumplan con las políticas y normas de seguridad de la información.

Guía de implementación

El cumplimiento técnico se evalúa mediante herramientas independientes que generan informes técnicos para ser interpretados por expertos. Alternativamente, el ingeniero puede realizar comprobaciones manuales (usando software si es necesario).

Se debe tener cuidado al realizar pruebas de penetración o pruebas de vulnerabilidad, pueden afectar la seguridad del sistema. Tales pruebas deben ser organizadas, registradas y repetidas.

Cualquier verificación del cumplimiento técnico solo debe ser realizada por o bajo la supervisión de personal calificado y autorizado.

Información adicional

Las auditorías de cumplimiento técnico incluyen sistemas de monitoreo en diseño o implementación para garantizar que los controles de hardware y software se implementen correctamente. Este tipo de prueba de cumplimiento requiere experiencia técnica.

Las pruebas de cumplimiento también cubren, por ejemplo, las pruebas de penetración y las pruebas de vulnerabilidad, que pueden ser realizadas por expertos independientes contratados para este fin.

Pueden ayudar a detectar vulnerabilidades del sistema y mejorar el rendimiento de los controles para evitar el acceso no autorizado debido a estas vulnerabilidades.

Las pruebas de penetración o las pruebas de vulnerabilidad proporcionan una instantánea de un sistema en un momento determinado. Este diagrama muestra solo una parte del sistema probado durante el test de penetración.

Las pruebas de penetración y la evaluación de vulnerabilidad no sustituyen a la evaluación de riesgos.

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

3.1. Descripción del escenario y evaluadores

Se hizo uso del escenario de dos empresas (CMS, CIAUTO) a evaluar, con el instrumento correspondiente para la ISO/IEC 27002, donde se formó una comparación técnica de los procesos y documentación establecida por cada empresa y se lo contrastará con cada uno de los puntos establecidos en la POLÍTICA DE SEGURIDAD INFORMÁTICA.

Por parte de la empresa Ciudad de Auto CIAUTO Cía. Ltda. el evaluador, será el coordinador del proceso de manufactura y está al tanto de todos los procedimiento y documentación del proceso.

De la empresa CMS, a evaluar, será el asistente 1 de desarrollo de software quien está a cargo de los procedimientos y de documentación necesaria para los diferentes procesos.

3.2. Presentación de los instrumentos

Para la aplicación de la evaluación a cada proceso de TI de las empresas (CMS, CIAUTO), se realizó la siguiente hoja de chequeo, donde se detalla los objetivos y controles correspondientes, a los cuales se les dará una calificación dependiendo del criterio de cada evaluador conforme al estado actual de procedimientos y documentación que mantenga cada una de las organizaciones.

La siguiente tabla muestra la hoja de chequeo proporcionada por la ISO 27002 la cual suministra un marco sólido y flexible para que las organizaciones evalúen la seguridad de la información de manera efectiva, adaptándose a sus necesidades específicas y promoviendo la mejora continua en los procesos necesarios existentes, no documentados y por aplicar.

Tabla N 10: objetivos de control y controles ISO/IEC 27002

ISO/IEC 27002, 23 OBJETIVOS DE CONTROL Y 70 CONTROLES		
ISO 27002 Contro-les	**Descripción**	**Sta-tus**
a) Política de seguridad de la información		
*	Política para la seguridad de la información	
*	Revisión de la política de seguridad de la información	
b) Dispositivos móviles y teletrabajo		
*	Política de dispositivos móviles	
*	Teletrabajo	
c) Durante el empleo		
*	Sensibilización, educación y formación en materia de seguridad de la infor-mación	
*	Cese o cambio de responsabilidades laborales	
d) Responsabilidad de los activos		
*	Inventario de activos y otros activos asociados	
*	Uso aceptable de los activos	
*	Devolución de activos	
e) Clasificación de la información		
*	Clasificación de la información	
*	Etiquetado de la información	
*	Uso aceptable de la información y otros activos asociados.	
f) Manejo de los medios de almacenamiento		
*	Medios de almacenamiento	
g) Requisitos empresariales del control de acceso		
*	Control de acceso	
h) Gestión del acceso de los usuarios		
*	Registro y baja de usuarios	
*	Derechos de acceso	
*	Derecho de accesos privilegiado	
*	Información de autenticación	
i) Control de acceso al sistema y a las aplicaciones		
*	Restricción de acceso a la información	
*	Autenticación segura	
*	Sistema de gestión de contraseñas	
*	Uso de programas de utilidad privilegiados	
*	Acceso al código fuente	
j) Controles criptográficos		
*	Uso de la criptografía	
k) Zonas seguras		
*	Parámetros de seguridad física	
*	Entrada física	
*	Asegurar las oficinas, salas e instalaciones	
*	Protección contra las amenazas físicas y medioambientales	
l) Seguridad en los equipos		
*	Ubicación y protección de los equipos	
*	Seguridad del cableado	

*	Mantenimiento de los equipos
*	Seguridad de los activos fuera de las instalaciones
*	Eliminación segura y reutilización de equipos
*	Dispositivos de punto final del usuario
*	Escritorio y pantalla despejados
m) Protección contra el malware	
*	Controles contra el malware
n) Copia de seguridad	
*	Información de respaldo
*	Realización y frecuencia del respaldo
o) Registro y control	
*	Registro
*	Registro de administración y operación
*	Sincronización de relojes
p) Control de software operativo	
*	Instalación de software es sistemas operativos
*	Gestión de vulnerabilidades técnicas
*	Restricción en la instalación del software.
q) Consideración sobre la auditoria de los sistemas de información	
*	Protección de los sistemas de información durante la auditoria
r) Gestión de la seguridad de red	
*	Seguridad en las redes
*	Seguridad en los servicios de red
*	Segregación de redes
s) Intercambios de información	
*	Transferencia de información
*	Acuerdos de confidencialidad y no divulgación
t) Seguridad en los procesos de desarrollo y apoyo	
*	Ciclo de vida de desarrollo seguro
*	Gestión del cambio
*	Arquitectura de sistemas seguros y principios de ingeniería
*	Separación de entornos de desarrollo, pruebas y producción
*	Desarrollo externalizado
*	Pruebas de seguridad en el desarrollo y la aceptación
u) Gestión de incidentes y continuidad de la seguridad de la información	
*	Planificación y preparación de la gestión de incidentes de seguridad
*	Informe de eventos de seguridad de la información
*	Evaluación y decisión sobre los eventos
*	Respuesta a los incidentes de seguridad de la información
*	Aprender de los incidentes de seguridad de la información
*	Recogida de pruebas
*	Seguridad de la información durante la interrupción
*	Preparación de las TIC para la continuidad de la actividad
v) Cumplimiento de los requisitos legales y contractuales	
*	Requisitos legales, reglamentarios y contractuales
*	Derechos de propiedad intelectual
*	Privacidad y protección de la información personal
w) Revisiones de la seguridad de la información	
*	Revisión independiente de la seguridad de la información

*	Cumplimiento de las políticas y normas de seguridad	
*	Revisión de la conformidad técnica.	

Fuente. ControlesISO27002

Para los criterios de evaluación de cada uno de los controles se tomó en cuenta la siguiente tabla de ponderación, el cual dependerá del estado en que se encuentra aplicado cada uno de los controles o si es necesario o no para la organización.

Tabla N 11: ponderación para evaluar los controles ISO/IEC 27002

Codigos Status	Significado
D	El control se documentó e implementó
MD	El Control se lleva a cabo y el proceso debe ser documentado para asegurar la repetitividad del proceso y mitigar los riesgos.
RD	El control no cumple las normas y debe ser re-diseñado para cumplir con las normas
PNP	El proceso no está en su lugar / no implementa-do. (Control requeridos ni documentado ni imple-mentado)
NA (Not Applicable)	El control no es aplicable para la empresa ni para el negocio

Fuente. ControlesISO27002

A continuación, se mostrará los resultados de las evaluaciones realizadas por los evaluadores de las organizaciones (CMS, CIAUTO).

CIAUTO

Cantidad	Codigos Status	Significado	Contribution %
31	D	El control se documentó e implementó	44%
24	MD	El Control se lleva a cabo y el proceso debe ser documentado para asegurar la repetibilidad del proceso y mitigar los riesgos.	34%
8	RD	El control no cumple las normas y debe ser rediseñado para cumplir con las normas	11%
2	PNP	El proceso no está en su lugar / no implementado. (Control requeridos ni documentado ni implementado)	3%
5	NA (Not Applicable)	El control no es aplicable para la empresa ni para el negocio	7%
70			

Para Ciauto, se puede interpretar que el 93% de la política es aplicable y aceptable, teniendo en cuanta que al contar con la ISO 9001 2015 implementada y en mejora continua, de los 70 controles, tienen implementados 31 dentro de la organización, también 24 controles deben ser documentados para formar parte de la implementación, 8 controles no cumplen las normas de la política y 2 no están implementados, los cuales deben tener un proceso adaptabilidad en estructura y contenido y aprobar como controles implementados.

CMS

Cantidad	Codigos Status	Significado	Contribution %
44	D	El control se documentó e implementó	63%
25	MD	El Control se lleva a cabo y el proceso debe ser documentado para asegurar la repetibilidad del proceso y mitigar los riesgos.	36%
1	RD	El control no cumple las normas y debe ser rediseñado para cumplir con las normas	1%
0	PNP	El proceso no está en su lugar / no implementado. (Control requeridos ni documentado ni implementado)	0%
0	NA (Not Applicable)	El control no es aplicable para la empresa ni para el negocio	0%
70			

CMS al ser una empresa de desarrollo de software mantiene estándares y controles de calidad que, al ser evaluados con la política de seguridad, tienen el 100% de aplicabilidad de los 70 controles, por lo cual mantienen 44 controles documentos e implementados, también 25 controles deben ser debidamente documentados para ser implementados completamente y 1 control que debe revisarse su estructura y contenido para ser parte de la aplicación de la política.

3.3. Sugerencias de parte del evaluador experto

- Es importante realizar evaluaciones regulares de seguridad, actualizar las políticas de autenticación y brindar capacitación continua al personal.
- Implementar políticas de seguridad claras y comunicarlas a los empleados, utilizar tecnologías de cifrado y autenticaciones robustas, y establecer protocolos para el manejo y transporte seguro de los activos fuera de las instalaciones. Además, se deben realizar evaluaciones periódicas de seguridad y brindar capacitación continua al personal sobre las mejores prácticas de seguridad.
- Realizar evaluaciones periódicas de seguridad, implementar soluciones de monitoreo y detección de vulnerabilidades, y establecer procedimientos para la corrección y mitigación de riesgos. Además, se deben establecer mecanismos de seguimiento y actualización para estar al tanto de las nuevas vulnerabilidades y parches de seguridad disponibles.
- Es establecer un proceso claro y documentado para identificar, proteger y gestionar los derechos de propiedad intelectual en el ámbito de las TIC. Esto implica la implementación de medidas de seguridad, como registros de patentes y marcas registradas, acuerdos de confidencialidad y políticas de protección de la propiedad intelectual. Además, es importante capacitar al personal sobre la importancia de respetar y salvaguardar estos derechos.
- Es fundamental desarrollar políticas claras y detalladas en varias áreas clave para garantizar la seguridad de la información y la

efectividad operativa. Se debe crear una política de dispositivos móviles y políticas de teletrabajo completas que aborden el acceso remoto a sistemas y datos corporativos. También es crucial documentar el proceso de gestión de responsabilidades en caso de cese o cambio de roles laborales, así como el proceso de inventario de activos, especificando los pasos a seguir y las responsabilidades.

- Además, se deben documentar detalladamente las reglas y políticas sobre el uso aceptable de los activos de la organización y establecer un esquema de clasificación de información claro y estructurado. Los procedimientos para el etiquetado de información deben ser desarrollados con detalle, y es importante simplificar y clarificar estos procedimientos para facilitar su implementación y cumplimiento.

CONCLUSIONES

- La identificación de elementos teóricos y metodológicos en la norma ISO/IEC 27002 revela un marco robusto para la gestión de la seguridad de la información. Teóricamente, la norma se basa en principios fundamentales de confidencialidad, integridad y disponibilidad, que son esenciales para proteger los activos informáticos de las organizaciones. Metodológicamente, la ISO/IEC 27002 proporciona directrices detalladas y controles específicos que abarcan diversos aspectos de la seguridad, desde la gestión de activos y control de accesos hasta la criptografía y la seguridad física. La norma enfatiza la importancia de la adaptación contextual, permitiendo a las organizaciones personalizar los controles según sus necesidades específicas y riesgos identificados. Además, promueve un ciclo de mejora continua mediante la implementación de políticas, evaluaciones periódicas y capacitaciones constantes. En conjunto, la ISO/IEC 27002 no solo establece un estándar de seguridad, sino que también ofrece un enfoque sistemático y adaptable para gestionar eficazmente la seguridad de la información en un entorno dinámico y en constante evolución.

- La identificación del estado actual de la organización y la evaluación de riesgos bajos, medios y altos son pasos críticos para la efectiva implementación y revisión de los controles de la norma ISO/IEC 27002. Este proceso permite a la organización entender su postura actual de seguridad y determinar las áreas que requieren atención prioritaria. La categorización de riesgos según su nivel de severidad facilita la asignación de recursos y esfuerzos donde son más necesarios, asegurando que los controles sean tanto eficaces como eficientes. Además, esta evaluación continua de riesgos ayuda a adaptar y mejorar los controles existentes, promoviendo una cultura de mejora constante en la seguridad de la información. Al identificar y mitigar los riesgos altos de manera proactiva, y al gestionar adecuadamente los riesgos medios y bajos, las organizaciones pueden fortalecer su resiliencia frente a amenazas potenciales. En

definitiva, este enfoque sistemático y estructurado asegura que la organización no solo cumpla con la norma ISO/IEC 27002, sino que también mantenga una postura de seguridad robusta y adaptable en un entorno en constante cambio.

- La elaboración de un plan de contingencia para la mitigación de los riesgos identificados en la matriz es esencial para fortalecer la resiliencia de la organización frente a incidentes de seguridad. Este plan debe basarse en un análisis exhaustivo de los riesgos bajos, medios y altos, priorizando las acciones necesarias para minimizar su impacto. La integración de los controles recomendados por la norma ISO/IEC 27002 asegura que las medidas adoptadas sean efectivas y alineadas con las mejores prácticas internacionales. Además, la presentación de una política de seguridad informática fundamentada en estas normas y estándares técnicos proporciona un marco claro y coherente para gestionar la seguridad de la información. Esta política debe comunicar claramente los roles y responsabilidades, así como los procedimientos y protocolos a seguir, garantizando la comprensión y el cumplimiento por parte de todo el personal. En conjunto, el plan de seguridad de la información propuesto y la política de seguridad sólida no solo mejoran la capacidad de respuesta ante incidentes, sino que también promueven una cultura organizacional centrada en la seguridad y la protección de los activos informáticos.

- La evaluación de las políticas de seguridad en Ciauto y CMS revela diferentes niveles de aplicabilidad e implementación de los controles de la norma ISO/IEC 27002. Para Ciauto, el 93% de la política es aplicable y aceptable, con 31 de los 70 controles ya implementados, 24 controles que necesitan ser documentados, 8 que no cumplen las normas y 2 que requieren adaptación. Esto indica un buen progreso, pero también resalta áreas críticas que necesitan atención para alcanzar un cumplimiento total. En contraste, CMS, como empresa de desarrollo de software, muestra un 100% de aplicabilidad de los controles, con 44 ya documentados e implementados, 25 que requieren documentación y solo 1 control que

necesita revisión. Esta diferencia sugiere que CMS está mejor posicionado en términos de cumplimiento de los estándares de seguridad. En conjunto, ambos casos subrayan la importancia de la documentación, la adaptación y la revisión continua para asegurar que todas las políticas de seguridad estén alineadas con los estándares ISO/IEC 27002, promoviendo así una gestión integral y efectiva de la seguridad de la información.

RECOMENDACIONES

- Para futuros trabajos en la implementación de una política de seguridad basada en ISO/IEC 27002, es esencial adoptar un enfoque sistemático y continuo. Primero, realizar un análisis exhaustivo del estado actual de la seguridad de la información en la organización para identificar brechas y áreas de mejora. Luego, involucrar a todas las partes interesadas, desde la alta dirección hasta los empleados, para asegurar una comprensión y compromiso común con la política. Es crucial documentar detalladamente todos los controles y procedimientos, asegurando que sean claros y accesibles. Además, establecer un programa de capacitación continua para el personal, enfocado en las mejores prácticas de seguridad y el cumplimiento de los controles establecidos. Implementar mecanismos de monitoreo y auditoría regulares para evaluar la efectividad de los controles y realizar ajustes necesarios. Finalmente, fomentar una cultura de mejora continua, revisando y actualizando la política de seguridad periódicamente para adaptarse a nuevos riesgos y cambios tecnológicos, asegurando así una protección robusta y sostenible de la información.

- Es fundamental establecer políticas claras y documentadas que definan el uso aceptable de la información y otros activos asociados. Se recomienda realizar revisiones periódicas de estas políticas, documentando adecuadamente el proceso. Si durante la revisión se identifica que el control actual no cumple con las normas, es esencial rediseñarlo para cumplir con los requisitos establecidos. Esto implica actualizar los procedimientos, asegurarse de que se sigan los protocolos adecuados y brindar la orientación necesaria a los empleados en relación con las responsabilidades laborales que están cesando o cambiando. Además, se deben implementar medidas de protección contra amenazas físicas y medioambientales, también documentadas adecuadamente. Para garantizar la efectividad de estas medidas, se recomienda realizar evaluaciones regulares de seguridad, actualizar las políticas de

autenticación y proporcionar capacitación continua al personal sobre las mejores prácticas de seguridad.

- Es fundamental establecer procedimientos claros para registrar actividades clave, utilizando herramientas y sistemas adecuados, y capacitar al personal en la importancia de mantener registros precisos y actualizados. Además, se deben realizar auditorías regulares para verificar el cumplimiento y corregir cualquier desviación identificada. Para garantizar la seguridad de manera proactiva, se recomienda realizar evaluaciones periódicas de seguridad, implementar soluciones de monitoreo y detección de vulnerabilidades, y establecer procedimientos para la corrección y mitigación de riesgos. Además, se deben establecer mecanismos de seguimiento y actualización para estar al tanto de las nuevas vulnerabilidades y parches de seguridad disponibles. Asimismo, es importante implementar firewalls, sistemas de detección y prevención de intrusiones, y controles de acceso adecuados. Estas medidas deben complementarse con evaluaciones periódicas de seguridad, actualizaciones de políticas de seguridad de red y capacitación continua del personal en las mejores prácticas de seguridad. Para asegurar la resiliencia empresarial, es crucial invertir en infraestructura y soluciones tecnológicas que permitan garantizar la continuidad de la actividad en situaciones adversas. Esto implica implementar medidas de seguridad como copias de seguridad regulares y sistemas de recuperación ante desastres, así como asegurar una conectividad confiable y estable.

BIBLIOGRAFÍA

Behar, C., Jorge, S., & Jorge, P. (2021). Epistemología do método científico: A técnica de entrevista. *Conhecendo Online*, *7*(1), Article 1.

Casa, A. C. L., Gavilánez, M. L. G., Caiza, C. C. C., & Moreano, J. A. C. (2021). Importancia de políticas de seguridad Informática de acuerdo a las ISO 27001 para pequeñas y medianas empresas del Ecuador. *Ciencias de la Ingeniería y Aplicadas*, *5*(2), Article 2.

Cevallos Jarro, H. Y. C. (s. f.). *DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE TICS DEL INSTITUTO TECNOLÓGICO SUPERIOR CENTRAL TÉCNICO, BASADO EN LA NORMA DE SEGURIDAD ISO/IEC 27002:2013*.

CSI Consultores en Seguridad de la Información. (s. f.). Recuperado 14 de junio de 2024, de https://www.csinfo.com.mx/

Enríquez, Á. S. C., Guijarro, J. V. H., & Cárdenas, C. A. G. (2022). Pruebas de penetración para la seguridad informática al servidor web del laboratorio de ciberseguridad en la Universidad Politécnica Estatal del Carchi, 2021. *SATHIRI*, *17*(2), Article 2. https://doi.org/10.32645/13906925.1138

Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., & Saltos-Gómez, J. A. (2018). La seguridad informática y la seguridad de la información. *Polo del Conocimiento*, *2*(12), 145. https://doi.org/10.23857/pc.v2i12.420

Gestión de vulnerabilidades. (2024). https://www.digicert.com/es/faq/vulnerability-management/what-is-the-difference-between-viruses-worms-and-trojan-horses

Guadalupe, G. D., & Concepción, G. D. (2020). *Metodología de la investigación*. Grupo Editorial Patria.

Hernández-Sampieri, D. R. (2018). *METODOLOGÍA DE LA INVESTIGACIÓN: LAS RUTAS CUANTITATIVA, CUALITATIVA Y MIXTA*.

ISOTools Excellence. (s. f.). ISO 27001. *ISOTools*. Recuperado 14 de junio de 2024, de https://isotools.org/isotools/normas/sistema-de-gestion-de-riesgos-y-seguridad/iso-27001/

Li, L., Berki, E., Helenius, M., & Ovaska, S. (2014). Towards a contingency approach with whitelist- and blacklist-based anti-phishing applications: What do usability tests indicate? *Behaviour & Information Technology*, *33*(11), 1136-1147. https://doi.org/10.1080/0144929X.2013.875221

Recognizing and Avoiding Spyware | CISA. (2009, noviembre 19). https://www.cisa.gov/news-events/news/recognizing-and-avoiding-spyware

Rhodes-Ousley, M. (s. f.). Information Security The Complete Reference. *Information Security*.

Richet, J.-L. (2013). From Young Hackers to Crackers. *International Journal of Technology and Human Interaction*, *9*, 53-62. https://doi.org/10.4018/jthi.2013070104

Rodríguez, C. R., Oré, J. L. B., & Vargas, D. E. (2021). *Las variables en la metodología de la investigación científica*. 3Ciencias.

Roque Hernández, R. V., & Juárez Ibarra, C. M. (2018). Awareness and Training to Increase Cyber-Security in University Students. *PAAKAT: Revista de Tecnología y Sociedad*, *8*(14), 1-13. https://doi.org/10.32870/Pk.a8n14.318

Santos-Olmo, A., Sánchez, L. E., Álvarez, E., Rosado, D. G., & Fernandez-Medina, E. (2020). Revisión Sistemática de Análisis de Riesgos Asociativos y Jerárquicos. Periodo 2014 – 2019. En V. Gauthier-Umaña, R. A. Méndez-Romero, & J. Ramió Aguirre (Eds.), *Seguridad Informática. X Congreso Iberoamericano, CIBSI 2020*. Universidad del Rosario. https://doi.org/10.12804/si9789587844337.13

Velepucha Sánchez, M. A., Morales Carrillo, J., & Pazmiño Campuzano, M. F. (2022). Análisis y evaluación de riesgos aplicados a la seguridad de la información bajo la norma ISO. *Informática y Sistemas: Revista de Tecnologías de la Informática y las Comunicaciones*, *6*(1), 63-78. https://doi.org/10.33936/isrtic.v6i1.4473

Villalobos Zamora, L. R. (2019). Enfoques y diseños de investigación social: Cuantitativos, cualitativos y mixtos. *Educación Superior*, *27*, 78-82. https://doi.org/10.56918/es.2019.i27.pp78-82

Yupanqui, J. R. A., Oré, S. B., & Unidad de Posgrado de la Facultad de Sistemas e Informática, Universidad Nacional Mayor de San Marcos (UNMSM), Av. Germán Amézaga s/n, Lima, Perú. (2017). Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento. *RISTI - Revista Ibérica de Sistemas e Tecnologías de Informação*, *25*, 112-134. https://doi.org/10.17013/risti.25.112-134

ANEXOS

Anexo 1. Evaluación realizada por el evaluador de la organización CIAUTO.

ISO/IEC 27002, 23 OBJETIVOS DE CONTROL Y 70 CONTROLES				
ISO 27002 Controles	**Descripción**	**Status**	**Observaciones**	**Recomendaciones**
a) Política de seguridad de la información				
*	Política para la seguridad de la información	D		
*	Revisión de la política de seguridad de la información	D		
b) Dispositivos móviles y teletrabajo				
*	Política de dispositivos móviles	MD	La falta de documentación puede ser un punto débil en el sistema de seguridad	Creación de una política de dispositivos móviles detallada
*	Teletrabajo	MD		Implementar políticas de teletrabajo completas que aborde aspectos como el acceso remoto a sistemas y datos corporativos
c) Durante el empleo				
*	Sensibilización, educación y formación en materia de seguridad de la información	D		
*	Cese o cambio de responsabilidades laborales	MD		Documentar el proceso para gestionar las respon-sabilidades en caso de cese o cambio de respon-sabilidades laborales
d) Responsabilidad de los activos				
*	Inventario de activos y otros activos asociados	MD		Es importante documentar de manera detallada el proceso de inventario de activos, incluyendo los pasos específicos a se-

				guir, las responsabilidades.
*	Uso aceptable de los activos	MD		Se debería documentar de manera detallada las reglas y políticas sobre el uso aceptable de los activos de la organización
*	Devolución de activos	MD	Aunque el control se está llevando a cabo, la necesidad de documentar el proceso es crucial para garantizar su consistencia y repetibilidad.	
e) Clasificación de la información				
*	Clasificación de la información	RD	No con las normas estándar de clasificación de información. La falta de un esquema de clasificación claro y específico puede dificultar la implementación efectiva del control.	Establecer un esquema de clasificación de información que sea claro, estructurado y fácil de entender.
*	Etiquetado de la información	RD	Falta de directrices claras sobre cómo etiquetar la información puede dificultar su correcta identificación y protección.	Se deberá desarrollar procedimientos detallados que abarquen todos los aspectos del etiquetado de la información.
*	Uso aceptable de la información y otros activos asociados.	D		
f) Manejo de los medios de almacenamiento				
*	Medios de almacenamiento	MD		Se recomienda simplificar y clarificar los procedimientos tanto como sea posible para facilitar su

				implementación y cumplimiento
g) Requisitos empresariales del control de acceso				
*	Control de acceso	D		
h) Gestión del acceso de los usuarios				
*	Registro y baja de usuarios	RD	El control propuesto carece de detalles específicos sobre cómo llevar a cabo estos procesos de manera efectiva.	Es fundamental desarrollar un procedimiento detallado y formal para el registro y la baja de usuarios.
*	Derechos de acceso	D		
*	Derecho de accesos privilegiado	D		
*	Información de autenticación	MD		Es de vital importancia detallar todos los procedimientos relacionados con la gestión de la información de autenticación secreta
i) Control de acceso al sistema y a las aplicaciones				
*	Restricción de acceso a la información	D		
*	Autenticación segura	D		
*	Sistema de gestión de contraseñas	D		
*	Uso de programas de utilidad privilegiados	MD		Es fundamental establecer políticas claras de autorización que definan quién tiene permiso para acceder y utilizar programas utilitarios.
*	Acceso al código fuente	NA (Not Applicable)		
j) Controles criptográficos				

*	Uso de la criptografía	MD		Se aplica el uso de criptografía especialmente en contraseñas de usuarios pero es importante llevar un registro de estas políticas
k) Zonas seguras				
*	Parámetros de seguridad física	MD		Documentar estas políticas para garantizará la consistencia en su aplicación y para proporcionar una referencia clara para el personal.
*	Entrada física	RD	Esto puede exponer a la empresa a riesgos de seguridad significativos, como accesos no autorizados a áreas sensibles o pérdida de información confidencial.	Es necesario revisar y mejorar los controles de acceso físico para garantizar que solo el personal autorizado pueda ingresar a las áreas seguras.
*	Asegurar las oficinas, salas e instalaciones	D		
*	Protección contra las amenazas físicas y medioambientales	D		
l) Seguridad en los equipos				
*	Ubicación y protección de los equipos	D		
*	Seguridad del cableado	D		
*	Mantenimiento de los equipos	D		
*	Seguridad de los activos fuera de las instalaciones	D		
*	Eliminación segura y reutilización de equipos	D		
*	Dispositivos de punto final del usuario	D		
*	Escritorio y pantalla despejados	RD	Al no existir políticas existe la posibilidad de que los empleados tengan baja productividad	Capacitar al personal sobre la importancia de mantener escritorios y pantallas despejados y de se-

				guir las políticas de seguridad establecidas.
m) Protección contra el malware				
*	Controles contra el malware	D		
n) Copia de seguridad				
*	Información de respaldo	D		
*	Realización y frecuencia del respaldo	D		
o) Registro y control				
*	Registro	MD		Se debe establecer un procedimiento claro para la revisión periódica de los registros de eventos
*	Registro de administración y operación	MD	Medidas de control de acceso y monitoreo para prevenir la manipulación no autorizada de los registros por parte de usuarios con privilegios.	
*	Sincronización de relojes	MD	Existe la necesidad de documentar los requisitos para la sincronización del tiempo y la obtención de una fuente de tiempo de referencia precisa.	
p) Control de software operativo				
*	Instalación de software es sistemas operativos	MD		Simplificar y clarificar los procedimientos tanto como sea posible para facilitar su implementación y cumplimiento.

*	Gestión de vulnerabilidades técnicas	RD	Este control abarca una amplia gama de consideraciones. Esta complejidad puede hacer que la implementación y el seguimiento del proceso sean desafiantes, especialmente si no están adecuadamente documentados y comunicados.	Documentar detalladamente todos los pasos y directrices relacionados con la gestión de vulnerabilidades técnicas y comunicarlos de manera efectiva a todo el personal relevante.
*	Restricción en la instalación del software.	MD	La instalación sin control puede llevar a vulnerabilidades y riesgos de seguridad significativos	
q) Consideración sobre la auditoria de los sistemas de información				
*	Protección de los sistemas de información durante la auditoria	MD	Es importante que las actividades de auditoría en sistemas operativos sean planificadas y acordadas cuidadosamente.	
r) Gestión de la seguridad de red				
*	Seguridad en las redes	D		
*	Seguridad en los servicios de red	D		
*	Segregación de redes	D		
s) Intercambios de información				
*	Transferencia de información	D		
*	Acuerdos de confidencialidad y no divulgación	D		
t) Seguridad en los procesos de desarrollo y apoyo				
*	Ciclo de vida de desarrollo seguro	NA (Not Applicable)		
*	Gestión del cambio	NA (Not Applicable)		
*	Arquitectura de sistemas seguros y principios de ingeniería	NA (Not Applicable)		
*	Separación de entornos de desarrollo, pruebas y pro-	NA (Not Applicable)		

	ducción			
*	Desarrollo externalizado	D		
*	Pruebas de seguridad en el desarrollo y la aceptación	D		
u) Gestión de incidentes y continuidad de la seguridad de la información				
*	Planificación y preparación de la gestión de incidentes de seguridad	MD		Realizar pruebas y simulacros periódicos para evaluar la efectividad del plan y los procedimientos de gestión de incidentes.
*	Informe de eventos de seguridad de la información	MD		Proporcionar formación continua sobre seguridad de la información a todos los empleados involucrados.
*	Evaluación y decisión sobre los eventos	MD	Es fundamental que cada evento de seguridad informático sea evaluado para determinar si debe clasificarse como un incidente.	
*	Respuesta a los incidentes de seguridad de la información	RD	Después de la resolución del incidente, es necesario realizar un cierre y registrar el evento.	Revisar y actualizar regularmente los procedimientos de respuesta a incidentes para garantizar su eficacia.
*	Aprender de los incidentes de seguridad de la información	PNP	La información obtenida del análisis proporciona una valiosa experiencia que puede utilizarse para mejorar los controles.	Implementar un proceso formal para aprender de los incidentes de seguridad de la información
*	Recogida de pruebas	RD	Recoger pruebas es fundamental para respaldar la investigación.	Realizar evaluaciones periódicas de los procedimientos de recogida de pruebas para identificar áreas de mejora.

*	Seguridad de la información durante la interrupción	MD		Realizar pruebas y simula-cros periódicos
*	Preparación de las TIC para la continuidad de la acti-vidad	MD		Proporcionar formación y capacitación regular al personal sobre las mejores prácticas de seguridad de la información
v) Cumplimiento de los requisitos legales y contractuales				
*	Requisitos legales, reglamentarios y contractuales	D		
*	Derechos de propiedad intelectual	D		
*	Privacidad y protección de la información personal	D		
w) Revisiones de la seguridad de la información				
*	Revisión independiente de la seguridad de la informa-ción	PNP	La implementación de revisiones independientes es Importan te para garan-tizar que los controles, políticas y procedimientos estén alineados con los estándares y requisitos.	Se debería designar un equipo interno o contratar a una entidad externa para llevar a cabo las revisiones periódicas.
*	Cumplimiento de las políticas y normas de seguridad	MD		Los coordinadores deben revisar regularmente los procedimientos de seguri-dad y estar abiertos a su-gerencias.
*	Revisión de la conformidad técnica.	MD	Es crucial que las pruebas de cumplimiento técnico sean realizadas únicamen-te por personal calificado y autorizado.	

Cantidad	Códigos Status	Significado	Contribution %
31	**D**	El control se documentó e implementó	**44%**
24	**MD**	El Control se lleva a cabo y el proceso debe ser documentado para asegurar la repetibilidad del proceso y mitigar los riesgos.	**34%**
8	**RD**	El control no cumple las normas y debe ser rediseñado para cumplir con las normas	**11%**
2	**PNP**	El proceso no está en su lugar / no implementado. (Control requeridos ni documentado ni implementado)	**3%**
5	**NA (Not Applicable)**	El control no es aplicable para la empresa ni para el negocio	**7%**
70			

Anexo 2. Evaluación realizada por el evaluador de la organización CMS.

ISO/IEC 27002, 23 OBJETIVOS DE CONTROL Y 70 CONTROLES				
ISO 27002 Controles	**Descripción**	**Status**	**Observaciones**	**Recomendaciones**
a) Política de seguridad de la información				
*	Política para la seguridad de la información	D		
*	Revisión de la política de seguridad de la información	MD	La revisión de la política de seguridad de la información es un paso crucial para evaluar si cumple con las normas y requisitos establecidos. Si se identifica que el control actual no cumple con las normas, es necesario rediseñarlo para asegurar el cumplimiento normativo	Se recomienda realizar revisiones periódicas de la política de seguridad de la información, documentando adecuadamente el proceso. Si se encuentra que el control actual no cumple con las normas, es fundamental rediseñarlo para cumplir con los requisitos establecidos.
b) Dispositivos móviles y teletrabajo				
*	Política de dispositivos móviles	D		
*	Teletrabajo	MD		
c) Durante el empleo				
*	Sensibilización, educación y formación en materia de seguridad de la información	D		

*	Cese o cambio de responsabilidades laborales	MD	el control actual no cumple con las normas, es necesario rediseñarlo para asegurar el cumplimiento normativo durante el proceso de cese o cambio de responsabilidades laborales.	Si se identifica que el control actual no cumple con las normas, es esencial rediseñarlo para cumplir con los requisitos establecidos. Esto implica revisar y actualizar los procedimientos, asegurarse de que se sigan los protocolos adecuados y brindar la orientación necesaria a los empleados en relación con las responsabilidades laborales que están cesando o cambiando.
d) Responsabilidad de los activos				
*	Inventario de activos y otros activos asociados	D		
*	Uso aceptable de los activos	MD		
*	Devolución de activos	D		
e) Clasificación de la información				
*	Clasificación de la información	MD		
*	Etiquetado de la información	D		
*	Uso aceptable de la información y otros activos asociados.	MD	El uso aceptable de la información y otros activos asociados es fundamental para garantizar la integridad y seguridad de los recursos de la organización	Se recomienda establecer políticas claras y documentadas que definan el uso aceptable de la información y otros activos asociados. Si se encuentra que el control actual no cumple con las normas, es fundamental rediseñarlo para cumplir con los requisitos establecidos y promover un uso responsable de los activos
f) Manejo de los medios de almacenamiento				

*	Medios de almacenamiento	D		
g) Requisitos empresariales del control de acceso				
*	Control de acceso	MD		
h) Gestión del acceso de los usuarios				
*	Registro y baja de usuarios	D		
*	Derechos de acceso	MD		
*	Derecho de accesos privilegiado	D		
*	Información de autenticación	MD		
i) Control de acceso al sistema y a las aplicaciones				
*	Restricción de acceso a la información	D		
*	Autenticación segura	MD	La autenticación segura es esencial para garantizar la identidad y acceso adecuado a sistemas y recursos.	es importante realizar evaluaciones regulares de seguridad, actualizar las políticas de autenticación y brindar capacitación continua al personal
*	Sistema de gestión de contraseñas	D		
*	Uso de programas de utilidad privilegiados	MD		
*	Acceso al código fuente	D		
j) Controles criptográficos				
*	Uso de la criptografía	MD		
k) Zonas seguras				
*	Parámetros de seguridad física	D		
*	Entrada física	MD		
*	Asegurar las oficinas, salas e instalaciones	D		

*	Protección contra las amenazas físicas y medioambientales	MD	La protección contra las amenazas físicas y medioambientales es fundamental para salvaguardar los activos y la continuidad de las operaciones de una organización	Se recomienda implementar medidas de protección contra amenazas físicas y medioambientales, documentando adecuadamente el proceso. Si se encuentra que el control actual no cumple con las normas, es fundamental rediseñarlo para cumplir con los requisitos establecidos.
l) Seguridad en los equipos				
*	Ubicación y protección de los equipos	D		
*	Seguridad del cableado	MD		
*	Mantenimiento de los equipos	D		
*	Seguridad de los activos fuera de las instalaciones	MD	La seguridad de los activos fuera de las instalaciones es crucial para proteger la integridad y confidencialidad de la información y recursos de una organización	implementar políticas de seguridad claras y comunicarlas a los empleados, utilizar tecnologías de cifrado y autenticación robustas, y establecer protocolos para el manejo y transporte seguro de los activos fuera de las instalaciones. Además, se deben realizar evaluaciones periódicas de seguridad y brindar capacitación continua al personal sobre las mejores prácticas de seguridad
*	Eliminación segura y reutilización de equipos	D		
*	Dispositivos de punto final del usuario	MD		
*	Escritorio y pantalla despejados	D		
m) Protección contra el malware				

*	Controles contra el malware	D		
n) Copia de seguridad				
*	Información de respaldo	D		
*	Realización y frecuencia del respaldo	D		
o) Registro y control				
*	Registro	D		
*	Registro de administración y operación	MD	El registro de administración y operación es fundamental para mantener un seguimiento adecuado de las actividades y decisiones en una organización	Esto implica establecer procedimientos claros para registrar actividades clave, utilizar herramientas y sistemas adecuados, y capacitar al personal en la importancia de mantener registros precisos y actualizados. Además, se deben realizar auditorías regulares para verificar el cumplimiento y corregir cualquier desviación identificada
*	Sincronización de relojes	D		
p) Control de software operativo				
*	Instalación de software es sistemas operativos	D		
*	Gestión de vulnerabilidades técnicas	MD	La gestión de vulnerabilidades técnicas es esencial para identificar y abordar de manera efectiva las debilidades en los sistemas y tecnologías de una organización	realizar evaluaciones periódicas de seguridad, implementar soluciones de monitoreo y detección de vulnerabilidades, y establecer procedimientos para la corrección y mitigación de riesgos. Además, se deben establecer mecanismos de seguimiento y actualización para estar al tanto de las

				nuevas vulnerabilidades y parches de seguridad disponibles
*	Restricción en la instalación del software.	D		
q) Consideración sobre la auditoria de los sistemas de información				
*	Protección de los sistemas de información durante la auditoria	D		
r) Gestión de la seguridad de red				
*	Seguridad en las redes	D		
*	Seguridad en los servicios de red	MD	La seguridad en los servicios de red es esencial para proteger la integridad y confidencialidad de la información que circula a través de la red	implementar firewalls, sistemas de detección y prevención de intrusiones, y controles de acceso adecuados. Además, se deben realizar evaluaciones periódicas de seguridad, actualizar las políticas de seguridad de red y brindar capacitación continua al personal sobre las mejores prácticas de seguridad
*	Segregación de redes	D		
s) Intercambios de información				
*	Transferencia de información	D		
*	Acuerdos de confidencialidad y no divulgación	D		
t) Seguridad en los procesos de desarrollo y apoyo				

*	Ciclo de vida de desarrollo seguro	D		
*	Gestión del cambio	D		
*	Arquitectura de sistemas seguros y principios de ingeniería	MD	La arquitectura de sistemas seguros y los principios de ingeniería son fundamentales para garantizar la protección y confiabilidad de los sistemas de información	aplicar los principios de defensa en profundidad, utilizar técnicas de cifrado y autenticación adecuadas, y realizar pruebas de seguridad regulares. Además, se deben seguir estándares y mejores prácticas de ingeniería de software para desarrollar sistemas robustos y confiables
*	Separación de entornos de desarrollo, pruebas y producción	D		
*	Desarrollo externalizado	D		
*	Pruebas de seguridad en el desarrollo y la aceptación	D		
u) Gestión de incidentes y continuidad de la seguridad de la información				
*	Planificación y preparación de la gestión de incidentes de seguridad	D		
*	Informe de eventos de seguridad de la información	D		
*	Evaluación y decisión sobre los eventos	D		
*	Respuesta a los incidentes de seguridad de la información	D		
*	Aprender de los incidentes de seguridad de la información	D		
*	Recogida de pruebas	D		
*	Seguridad de la información durante la interrupción	D		

*	Preparación de las TIC para la continuidad de la actividad	D	La dependencia de la tecnología en los negocios y organizaciones es cada vez mayor, por lo que contar con sistemas y recursos tecnológicos confiables se ha vuelto crucial para mantener el funcionamiento ininterrumpido de las operaciones.	Es importante invertir en infraestructura y soluciones tecnológicas que permitan garantizar la continuidad de la actividad en situaciones adversas. Esto implica implementar medidas de seguridad, como copias de seguridad regulares y sistemas de recuperación ante desastres, así como asegurar una conectividad confiable y estable.
v) Cumplimiento de los requisitos legales y contractuales				
*	Requisitos legales, reglamentarios y contractuales	MD	Son aspectos críticos que se toman en cuenta al establecer controles y documentación adecuados en una organización. Estas obligaciones externas imponen ciertas responsabilidades y estándares que deben cumplirse para garantizar el cumplimiento normativo y contractual.	es importante realizar un análisis exhaustivo de las regulaciones aplicables y los acuerdos contractuales relevantes. Esto permitirá identificar los controles y documentación necesarios para cumplir con dichos requisitos
*	Derechos de propiedad intelectual	D	Para garantizar su protección, es fundamental implementar controles y documentar adecuadamente los activos de propiedad intelectual relacionados con las tecnologías de la información y comunicación.	Es establecer un proceso claro y documentado para identificar, proteger y gestionar los derechos de propiedad intelectual en el ámbito de las TIC. Esto implica la implementación de medidas de seguridad, como registros de patentes y marcas registradas, acuerdos de confidencialidad y políticas de protección de la propiedad intelectual. Además,

				es importante capacitar al personal sobre la importancia de respetar y salvaguardar estos derechos.
*	Privacidad y protección de la información personal	MD	La privacidad y protección de la información personal son aspectos fundamentales en el entorno actual. Garantizar un control adecuado y documentado en el manejo de la información personal es esencial para protegerla de manera efectiva y mitigar los riesgos asociados.	Para asegurar la privacidad y protección de la información personal, es importante establecer políticas y procedimientos claros que sean documentados y repetibles. Esto implica implementar medidas de seguridad, como encriptación de datos, acceso restringido y capacitación en la gestión adecuada de la información personal
w) Revisiones de la seguridad de la información				
*	Revisión independiente de la seguridad de la información	MD	La revisión independiente de la seguridad de la información es un aspecto clave para garantizar la integridad y protección de los datos. Mediante esta revisión, se obtiene una visión imparcial y experta de los controles de seguridad implementados, identificando posibles vulnerabilidades y riesgos.	Se recomienda realizar regularmente revisiones independientes de la seguridad de la información, documentando adecuadamente el proceso. Estas revisiones deben ser realizadas por profesionales especializados y externos a la organización, con el fin de asegu-

				rar una evaluación imparcial.
*	Cumplimiento de las políticas y normas de seguridad	MD	El cumplimiento de las políticas y normas de seguridad es esencial para mantener la integridad y confidencialidad de la información. Asegurar que se lleve a cabo un control adecuado y documentado en relación con las políticas y normas establecidas ayuda a garantizar un entorno seguro.	Se recomienda establecer procesos claros y documentados para asegurar el cumplimiento de las políticas y normas de seguridad. Esto implica la implementación de controles y medidas de seguridad adecuadas, así como la capacitación y concienciación del personal sobre las políticas y normas establecidas.
*	Revisión de la conformidad técnica.	RD	La revisión de la conformidad técnica es un proceso esencial para evaluar si los sistemas y tecnologías cumplen con las normas y estándares establecidos. Si el control actual no cumple con las normas, es necesario realizar un rediseño para garantizar la conformidad.	Se recomienda realizar revisiones periódicas de la conformidad técnica, documentando adecuadamente el proceso. Si se identifica que el control actual no cumple con las normas, es fundamental rediseñarlo para cumplir con los estándares establecidos

Cantidad	Códigos Status	Significado	Contribution %

44	**D**	El control se documentó e implementó	**63%**
25	**MD**	El Control se lleva a cabo y el proceso debe ser documentado para asegurar la repetibilidad del proceso y mitigar los riesgos.	**36%**
1	**RD**	El control no cumple las normas y debe ser rediseñado para cumplir con las normas	**1%**
0	**PNP**	El proceso no está en su lugar / no implementado. (Control requeridos ni documentado ni implementado)	**0%**
0	**NA (Not Applicable)**	El control no es aplicable para la empresa ni para el negocio	**0%**
70			