UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA INFORMÁTICA

Trabajo final de graduación para optar por el grado de Bachillerato en Ingeniería de Sistemas de Información

Propuesta para la protección de datos, basado en la norma ISO/IEC 27001, para la empresa Landergren Consulting Group, Ubicada en Guachipelín de Escazú

AUTOR

Andrey Mora Fonseca

TUTOR

Carlos Humberto Aguilar

San José, Costa Rica

ABRIL, 2023

Dedicatoria

A mis padres:

Su amor incondicional, su constante apoyo y su sacrificio han sido la fuerza impulsora detrás de cada paso que he dado en este viaje académico. Gracias por creer en mí, por alentarme en los momentos difíciles y por celebrar conmigo cada pequeño logro. Este logro no sería posible sin su constante guía y respaldo.

A mi hermana:

Tu apoyo inquebrantable a través de cada altibajo, siempre has estado a mi lado, compartiendo mis triunfos y consolándome en las derrotas. Tu presencia ha enriquecido mi camino y le ha dado sentido a cada paso que doy.

A mi novia:

Tu amor, paciencia y comprensión han sido mi roca durante esta travesía. Tus palabras de aliento, tus abrazos reconfortantes y tu presencia constante han iluminado incluso los días más oscuros. Gracias por ser mi inspiración, mi compañera de vida y por estar a mi lado en cada desafío que hemos enfrentado juntos.

Les dedico este trabajo con profundo agradecimiento y amor eterno. Son mi mayor motivación y la razón por la que nunca me rindo.

Agradecimientos

Quiero expresar mi más sincero agradecimiento a todas las personas e instituciones que contribuyeron de alguna manera a la realización de este trabajo de investigación.

En primer lugar, agradezco a mi directora de tesis, Olda Bustillos Ortega, por su orientación experta, su paciencia y su dedicación durante todo el proceso de investigación. Sus consejos y comentarios fueron fundamentales para dar forma a este trabajo y llevarlo a buen término.

También quiero expresar mi profundo agradecimiento a mi tutor, Carlos Aguilar Mora, por su invaluable asesoramiento y orientación a lo largo de este proyecto. Su experiencia y sabiduría fueron cruciales para superar los desafíos y alcanzar los objetivos propuestos.

Agradezco profundamente a mis padres, por su amor incondicional, su apoyo inquebrantable y su sacrificio para que yo pudiera alcanzar mis metas académicas. Su constante aliento y motivación han sido mi mayor impulso en este camino.

A mi novia y a mi hermana, les agradezco por su paciencia, comprensión y amor incondicional. Su presencia y apoyo emocional fueron fundamentales para mantenerme motivado durante los momentos más desafiantes de este proceso.

Además, quiero agradecer a mis amigos y seres queridos por su ánimo, su compañerismo y su apoyo en cada etapa de este viaje. Su amistad ha hecho que este camino sea mucho más llevadero y significativo.

Finalmente, agradezco a la empresa Landergren Consulting Group por proporcionarme los recursos y el entorno propicio para llevar a cabo esta investigación.

A todas las personas que de una u otra manera han contribuido a la realización de esta tesis, mi más sincero agradecimiento. Su colaboración y apoyo han sido invaluables y nunca serán olvidados.

Contenido

ILUSTRACIONES

TABLAS

Resumen Ejecutivo

La presente investigación se centró en el análisis de las políticas de seguridad de datos y la protección de la información del sistema contable de la empresa Landergren Consulting Group (LCG), con base en las normas ISO/IEC 27001. Se empleó un enfoque cuantitativo mediante encuestas y entrevistas a 20 empleados de LCG.

En cuanto a la restricción de navegación en internet, se observó la ausencia de incidentes significativos hasta la fecha, aunque se sugiere una revisión y actualización de las políticas para fortalecer la seguridad. Respecto al control de acceso y criptografía, se identificó la necesidad de implementar programas de capacitación para garantizar la plena comprensión y adherencia a las políticas de seguridad. En el control de credenciales y permisos, se destacó la importancia de desactivar cuentas de empleados de manera estructurada al abandonar la organización, así como la necesidad de evitar la práctica de compartir credenciales a través de canales no seguros. En relación con la seguridad en usuarios, se resaltó la importancia de implementar prácticas regulares de evaluación de contraseñas y abordar la ausencia de medidas para contrarrestar contraseñas débiles. En la seguridad en la red, se sugirió realizar evaluaciones de seguridad con mayor periodicidad para fortalecer la preparación ante posibles amenazas futuras. Finalmente, en el control y prevención de correos electrónicos, se destacó la necesidad de mejorar la educación sobre los riesgos asociados con correos electrónicos maliciosos.

Las recomendaciones incluyen la asignación de responsabilidades claras para la implementación de políticas de seguridad, la realización de programas de capacitación y la implementación de procedimientos específicos para garantizar la seguridad de la información en diferentes áreas.

Este resumen ejecutivo destaca la importancia de abordar las áreas identificadas para fortalecer la seguridad de datos y proteger la información del sistema contable de LCG, asegurando así la integridad y confidencialidad de los datos de la organización.

CAPÍTULO I: INTRODUCCIÓN

Planteamiento del Problema

La empresa Landergren Consulting Group (LCG), es un despacho de contadores encargado de hacer cierres fiscales y aperturas de cuentas para bancos, también se encarga de llevar la contabilidad de diferentes entidades y el área de recursos humanos. La entidad cuenta con 21 empleados laborando actualmente y se encuentra ubicada en Escazú, Guachipelín.

Descripción del Problema

- Uso incorrecto de navegación a internet por parte de los empleados: Al no tener restricciones de navegación, los empleados pueden entrar a páginas maliciosas, esto puede abrir una brecha de información y ser hackeados.
- Robo o divulgación, alteración y pérdida de información confidencial: No se cuenta con controles de seguridad, políticas, procedimientos, guías o directrices en la organización y esto ocasiona deficiencias en la gobernabilidad de la seguridad.
- Gestión inadecuada de permisos y credenciales: Debido a una gestión inadecuada de credenciales, las personas quienes ya no siguen en la organización pueden seguir usando su cuenta proporcionada por la empresa. Lo anterior provoca que, al no haber una buena gestión de credenciales, ello pueda permitir el robo de información de la empresa y de clientes.
- No existen políticas de seguridad de contraseñas de usuarios: Debido a la falta de políticas, las contraseñas son vulnerables a cualquier tipo de ataque, lo cual provoca, al ser contraseñas poco seguras, sea favorable sean atacados por un hacker para robar información.
- Inseguridad en la red: No se cuenta con una buena seguridad de la red para proteger los datos e información de la empresa, lo que puede provocar un posible ataque al sistema de la empresa.
- No existe un Control de Correo Electrónico y Prevención de Phishing: Al no tener un buen control de correo electrónico, los empleados pueden entrar a enlaces maliciosos y caer en un ataque de phishing.

Objetivo General

Diseñar una propuesta de mejora basada en la norma ISO/IEC 27001 para la seguridad de datos y la información del sistema contable de la empresa Landergren Consulting Group (LCG).

Objetivos específicos

- Crear la política de restricción de navegación a internet de acuerdo con la norma ISO/IEC 27001.
- Construir el procedimiento de las medidas para proteger y controlar los dispositivos que acceden a la información de acuerdo con la norma ISO/IEC 27001.
- Elaborar el procedimiento para la gestión de acceso de usuarios de acuerdo con la norma ISO/IEC 27001.
- Construir el procedimiento de seguridad de usuario para el control de acceso a sistema y aplicaciones de acuerdo con la norma ISO/IEC 27001.
- Analizar la protección de los datos y la información, de acuerdo con la norma ISO/IEC 27001.
- Elaborar medidas para el control de correo electrónico y prevención de phishing, de acuerdo con la norma ISO/IEC 27001

Justificación

Debido a la importancia de la seguridad de la información en el entorno empresarial actual, el estudio de la protección de datos e información en los sistemas contables es fundamental. Ayuda a proteger datos críticos, garantizar el cumplimiento y mantener la confianza del cliente en un entorno de amenazas cibernéticas en constante evolución.

Los resultados de la investigación sobre la seguridad de los datos y la información en los sistemas contables pueden tener una amplia gama de beneficios, desde mejorar la seguridad y el cumplimiento normativo hasta mejorar la reputación empresarial y proteger la confianza de los clientes. Estos beneficios pueden tener un impacto positivo a nivel empresarial, así como a nivel social y ético.

Viabilidad técnica

La empresa ya cuenta con una infraestructura tecnológica establecida. Incluye servidores, sistemas de bases de datos, aplicaciones de software y redes de

comunicaciones. Esta infraestructura proporciona la base técnica para realizar auditorías de seguridad.

Se considera utilizar las normas ISO relacionadas con la seguridad de la información, como ISO 27001, pues proporcionan un marco reconocido internacionalmente para la gestión de la seguridad de la información.

Viabilidad operativa

Para llevar a cabo esta investigación de manera efectiva, se requiere conocimiento sólido en el campo de la seguridad de la información, esto incluye la comprensión de las mejores prácticas de seguridad, las amenazas cibernéticas comunes y las técnicas de mitigación.

Se debe ofrecer capacitaciones al personal de la empresa, para así puedan comprender y seguir las nuevas políticas y procedimientos de seguridad, esto para que los empleados puedan reconocer y responder a una posible amenaza. Es esencial documentar detalladamente las políticas y procedimientos de seguridad, además, comunicarlos efectivamente a todo el personal, para que estén bien informados de las medidas de seguridad de la empresa. Estas capacitaciones son parte de las recomendaciones brindadas en la investigación para obtener mejores prácticas de seguridad, pero no es incluida dentro del proyecto de graduación.

Viabilidad Económica

Costo de software: Incluye la adquisición o licenciamiento de herramientas de software especializados para llevar a cabo auditorías de seguridad, pruebas de penetración y análisis de riesgos.

Costo de hardware: Esto puede abarcar la compra de servidores de pruebas, dispositivos de seguridad y cualquier equipo necesario para realizar evaluaciones de seguridad.

Costos de Mantenimiento y Soporte: Se debe considerar los costos continuos de mantenimiento y soporte para las soluciones de seguridad implementadas, como actualizaciones de software y suscripciones a servicios de seguridad gestionados, cada cierto tiempo estimado se debe pagar a un técnico para que mantenga actualizado el software.

Costos de Documentación y Comunicación: La creación de documentación de políticas y procedimientos de seguridad, seria parte de las nuevas políticas y procedimientos por realizar en la propuesta del proyecto, así como la comunicación

interna sobre las medidas de seguridad, también tiene costos asociados, gastos como materiales de impresión.

Enseguida se muestra una tabla detallada con los costos económicos:

Tabla 1

Costos económicos

Nombre	Precio
pentesting - Prueba de penetración	Prueba gratuita temporal
Análisis de riegos	Ejecutado por mi persona
TotalAV – Antivirus PRO	Prueba gratuita
Almacenamiento nube AWS	Prueba gratuita
Cifrado de datos	Prueba gratuita
Mantenimientos y soporte del software	Los precios van de 10.000 a 20.000 colones dependiendo de la tarea por ejecutar
Ordenador principal Especificaciones: Intel Core i5 8 GB de RAM 1 T de almacenamiento	550.000 colones computadora propia
Servicio de conexión a internet fibra óptica Metrocom 300 GB	40.000 colones mensuales

Fuente: Elaboración Propia

Se utiliza versiones gratuitas, pues quien realiza este estudio no forma parte de la empresa y solo se utilizan para realizar el proyecto.

Viabilidad Legal

El desarrollo de la investigación para la seguridad de información en la empresa Landergren Consulting Group (LCG), debe cumplir con la legislación vigente en Costa Rica, adhiriéndose a las siguientes leyes:

Ley N° 4573 para reprimir y sancionar los delitos informáticos de la Asamblea Legislativa de la República de Costa Rica del año 200 según el análisis de la " Ley N° 4573 para reprimir y sancionar los delitos informáticos de la Asamblea Legislativa de la República de Costa Rica del año 2001", se determina el proyecto de investigación para la

seguridad de información, no viola ninguno de los mencionados artículos. Por lo tanto, se confirma la viabilidad legal del sistema en frente del ámbito legal.

Ley de Derechos de Autor 6683 por parte de la Asamblea Legislativa de la República de Costa Rica del año 1982, según el análisis de la “Ley de Derechos de Autor 6683 por parte de la Asamblea Legislativa de la República de Costa Rica del año 1982” se determina estar usando los debidos programas brindados de manera gratuita por las diferentes instituciones y las cuales son de uso educativo, por lo anterior esto no viola ninguno de los artículos mencionados, en consecuencia, se confirma la viabilidad legal del sistema ante la ley de derechos humanos.

Ley 8968 sobre la protección de la persona frente al tratamiento de sus datos personales Basado en el análisis de la " Ley 8968 sobre la protección de la persona frente al tratamiento de sus datos personales", se concluye: el proyecto de investigación para la seguridad de información, no inflige los requisitos legales establecidos en dicha ley. Esto garantiza que el sistema respeta la privacidad y protección de los datos personales de los empleados y clientes de Landergren Consulting Group (LCG), pues dicha información si usa con fines de la realización del proyecto, por tanto, se asegura su viabilidad legal y su conformidad con las disposiciones legales vigentes de la ley antes presentada.

Proyecciones

La investigación tiene como objetivo mejorar la seguridad de los datos en los sistemas de contables de la empresa, garantizar el cumplimiento normativo, proteger la reputación de la empresa y reducir los riesgos financieros asociados con los incidentes de seguridad. El alcance funcional abarca desde la evaluación de riesgos, hasta la implementación de políticas y procedimientos para el sistema. El alcance metodológico implica revisión documental, auditorías y entrevistas, el alcance tecnológico se evalúa y se recomienda soluciones tecnológicas para fortalecer la seguridad del sistema contable.

Alcance Funcional

La investigación para la seguridad de información de la empresa Landergren Consulting Group (LCG) se compone de los siguientes apartados:

Políticas de restricción de navegación a internet: Crear la política de restricción de navegación a internet de acuerdo con la norma ISO/IEC 27001, la cual abarque el control de acceso a las redes y a los servicios de red, bloqueando o restringiendo páginas de entretenimiento, los empleados solamente van a poder acceder al navegador con fines laborales.

Control de acceso y Criptografía: Construir el procedimiento de las medidas para proteger y controlar los dispositivos que acceden a la información de acuerdo con la norma ISO/IEC 27001, la cual abarca el uso de técnicas de cifrado para proteger la información en reposo y en tránsito, también privilegios que tienen los usuarios en cuanto a las aplicaciones y a la información.

Control de credenciales y permisos: Elaborar el procedimiento para la gestión de acceso de usuarios de acuerdo con la norma ISO/IEC 27001, se plantea el uso de la retirada o reasignación de los derechos de acceso a la plataforma a los empleados quienes dejan de trabajar en la empresa y evitar la información privada caiga en manos de la competencia.

Control de seguridad en usuarios: Construir el procedimiento de seguridad de usuario para el control de acceso al sistema y aplicaciones de acuerdo con la norma ISO/IEC 27001, se plantea elaborar contraseñas complejas con caracteres especiales, letras en mayúsculas, minúsculas y números, teniendo una longitud mínima de ocho dígitos, esto para obtener contraseñas más robustas y evitar hackeos.

Control de seguridad en la red: Analizar la protección de los datos y la información, de acuerdo con la norma ISO/IEC 27001, se plantea el uso de Firewalls, Control de Acceso a la Red (NAC), Detección y Prevención de Intrusiones (IDS/IPS), VPN (Redes Privadas Virtuales), Monitoreo y Registro.

Control y prevención de correo electrónico: Elaborar medidas para el control de correo electrónico y prevención de phishing, de acuerdo con la norma ISO/IEC 27001, la cual plantea el uso de filtrado de correo electrónico, Antivirus y Antimalware, Autenticación de Correo Electrónico (SPF, DKIM, DMARC), Políticas de Uso de Correo Electrónico, respuesta a incidentes de Phishing.

Alcance Metodológico

Realizar una evaluación exhaustiva de los riesgos de seguridad que enfrentan los sistemas contables. Esto incluye identificar amenazas, evaluar su probabilidad e impacto y priorizar los riesgos.

Realizar una auditoría de seguridad para evaluar la postura de seguridad actual de los sistemas contables. Esto implica revisar las configuraciones, políticas y procedimientos de seguridad existentes.

Desarrollar políticas y procedimientos de seguridad específicos para abordar las vulnerabilidades identificadas y cumplir con las mejores prácticas de seguridad de la información.

Implementar las medidas de seguridad recomendadas, estas pueden incluir configuración de firewall, sistemas de detección de intrusos, cifrado de datos y controles de acceso.

Alcance Tecnológico

Para fortalecer la seguridad, se utiliza herramientas y tecnologías de seguridad, como firewall, sistemas de detección de intrusiones (IDS/IPS), sistemas de prevención de intrusiones (IPS), encriptación de datos y software antivirus.

CAPÍTULO II: MARCO REFERENCIAL

En este capítulo se presenta una recopilación de términos y conceptos claves para la comprensión detallada de la estructura y funcionalidad de las herramientas desarrolladas en esta investigación. Estos términos no solo brindan a los lectores una base sólida de conocimiento, sino también les permiten obtener una perspectiva más crítica e informada al analizar y evaluar la investigación por realizar. Al familiarizarse con estos conceptos, el lector puede obtener una comprensión más precisa y profunda de los aspectos técnicos y teóricos involucrados en la presente investigación.

Un sistema contable es una estructura mediante la cual se registra todas las operaciones que hace una empresa para obtener sus datos contables y financieros. Es una manera de poder controlar los resultados de las transacciones y comprender el estado económico del negocio. Welink Accountants (2023) comenta:

> Para poder trabajar con un sistema contable hay que definir previamente las normas o pautas que se van a aplicar a la hora de controlar las operaciones de la empresa, así como para clasificar la información relativa a las gestiones contables y financieras. Esto es la manera en la que se llevan las cuentas de una empresa. (párr.3)

Según Welink Accountants (2023) cada empresa puede desarrollar el sistema de contabilidad que más se adecue a su manera de trabajar, pero en cualquier caso es fundamental cumpla con los siguientes requisitos:

- Comprensibilidad: Un sistema contable efectivo debe ser comprensible para todas las partes interesadas, desde expertos en finanzas hasta cualquier empleado de la empresa. La transparencia y claridad en los registros contables son esenciales para que cualquier persona, independientemente de su nivel de conocimiento en contabilidad, pueda entender fácilmente la situación financiera de la empresa. Los informes y registros contables deben estar redactados de manera clara y concisa, utilizando un lenguaje que sea fácilmente entendible para todos los usuarios. La comprensibilidad no solo facilita la toma de decisiones informadas por parte de los directivos, sino que también promueve la confianza y la transparencia dentro de la organización.
- Usabilidad: La usabilidad es un aspecto fundamental de cualquier sistema de contabilidad. Debe ser intuitivo y fácil de usar para que los empleados puedan registrar y acceder a los datos financieros de manera rápida y eficiente. Un sistema contable fácil de usar no solo ahorra tiempo, sino que también reduce

la probabilidad de errores humanos al ingresar datos. La información financiera debe estar organizada de manera lógica y accesible, lo que facilita a los usuarios encontrar la información relevante cuando la necesitan. La usabilidad también se relaciona con la capacidad del sistema para generar informes personalizados y análisis detallados, lo que permite a la empresa obtener insights valiosos para mejorar su rendimiento y tomar decisiones estratégicas.

- Fiabilidad: La fiabilidad es quizás el requisito más crítico de un sistema contable. Todos los datos que se registran y se utilizan en los informes financieros deben ser precisos y verificables. La información financiera inexacta o falsa puede llevar a decisiones empresariales erróneas que podrían tener consecuencias graves. Para garantizar la fiabilidad, es fundamental establecer controles internos sólidos y procesos de verificación rigurosos. Los datos deben ser consistentes y estar respaldados por documentos y transacciones reales. La integridad de los datos es esencial para la credibilidad de la empresa ante inversores, acreedores y otras partes interesadas. Un sistema contable confiable no solo cumple con las normativas legales y fiscales, sino que también establece una base sólida para la gestión financiera efectiva y el crecimiento sostenible de la empresa.

Según Welink Accountants (2023) el uso de estos sistemas para gestionar la contabilidad de una empresa, solo debería reportar beneficios, en cuanto es una solución para llevar a cabo una tarea necesaria. Pero la realidad es que el uso de un sistema contable también tiene algún inconveniente.

Ventajas de un sistema contable:

- Permite gestionar los gastos e ingresos de manera casi automática.
- Mantiene ordenada la actividad diaria para un mayor control.
- Detecta cualquier incidencia casi en el momento en que ocurra.
- Controla las pérdidas y ganancias.
- Permite una mejor gestión de los recursos al tener acceso a la información de manera permanente.

Desventajas de un sistema contabilidad:

- El principal inconveniente es el tiempo necesario para llevarlo a cabo, pues supone una tarea que ha de hacerse de manera diaria.

- Necesita contar con una persona formada en contabilidad para llevar a cabo esta tarea de manera segura.
- En caso de que no se sea riguroso o se introduzca algún dato erróneo el sistema deja de ser fiable. (párr.7)

Para proteger los datos privados almacenados en los sistemas contables, la seguridad informática es un pilar fundamental. En esta situación, es básico garantizar el acceso autorizado, proteger la integridad de los datos y mantener la confidencialidad. Es imprescindible tomar precauciones contra las amenazas cibernéticas, implementar un cifrado confiable y estar atento a posibles vulnerabilidades. Los datos vitales que respaldan las operaciones financieras deben mantenerse seguros para conservar la confianza de los clientes y partes interesadas en la confidencialidad e integridad de la información contable de la empresa. Esto sólo se puede lograr implementando estrategias efectivas de ciberseguridad. Según Araya, S. (2020). "La seguridad informática es esencial para proteger los datos confidenciales almacenados en un sistema contable. Esto incluye la protección contra el acceso no autorizado, la defensa de la integridad de los datos y la conservación de la confidencialidad." (párr.7)

Según Araya, S. (2020) esto se puede lograr mediante la implementación de medidas de seguridad adecuadas que ayuden a reducir el riesgo de robo de información, daños a los datos o cualquier otra amenaza a la seguridad. Enseguida se presenta recomendaciones para garantizar la seguridad de la información:

Establece una política de seguridad informática: La primera medida para garantizar la seguridad es establecer una política de resguardo de los datos informáticos, debe ser clara, detallada y conocida por todos los miembros de la organización; debe incluir reglas específicas sobre el uso y la protección de la data, así como las sanciones por incumplimiento.

Adquiere un sistema de seguridad de la información: El siguiente paso es la adquisición de un software de seguridad que incluya la instalación de firewalls, el uso de antivirus y otras herramientas para proteger los datos.

Implementa una formación adecuada: El adiestramiento es esencial para garantizar la seguridad de la información. Los usuarios deben recibir aprendizaje sobre las mejores prácticas de seguridad y los riesgos asociados con el uso de la información.

Usa contraseñas seguras: La primera línea de defensa es la password y se debe proteger conveniente. Por lo tanto, el primer objetivo va a ser crear una contraseña segura. En ese aspecto se debe buscar que mínimo tenga 10 caracteres. Aquí se debe incluir letras

mayúsculas y minúsculas, números y símbolos especiales. Eso sin olvidar que no se debe reutilizar para otras cuentas y se deben cambiar periódicamente.

Utiliza una solución de copia de seguridad: Las copias de seguridad son una forma de resguardar los datos en caso de producirse una falla en el sistema. Esto garantiza la información sea recuperable.

Para que sea seguro, un sistema contable debe contener las siguientes herramientas y características:

La autenticación de usuario según Lorenzo, J. (2022). “podemos definirla como un proceso de seguridad que evita que los usuarios no autorizados accedan a un dispositivo o red. Nos encontramos con un procedimiento de inicio de sesión donde una aplicación nos solicita nuestra contraseña para darnos acceso.” (párr.3). La autenticación de usuario garantiza el acceso a la red de esa aplicación a la cual se ingresa a través de una cuenta, no caiga en manos de los ciberdelincuentes.

Su forma de operar consiste en primer lugar en ingresar sus credenciales de inicio de sesión en una pantalla de inicio. donde se debe introducir el nombre de usuario y contraseña. La siguiente fase consiste en autenticar la información de inicio de sesión. Este proceso empieza cuando el servidor al que se intenta acceder recibe la información personalizada que se le envía. A continuación, dicha información se compara con las credenciales ingresadas y almacenadas con éxito en la base de datos. Después el ordenador aprueba el acceso si los datos coinciden con la base de datos o rechaza la solicitud si no son los correctos.

Gracias a la autenticación de usuario, la información ingresada para la verificación se aprueba o se rechaza. Si se rechaza la petición muestra un mensaje donde se dice que ha introducido información incorrecta o ha olvidado la contraseña. También dependiendo de la configuración, puede tener la oportunidad de iniciar otra solicitud o se bloquee el acceso a esa cuenta. En ocasiones, además ofrecen una opción para poder recuperar esa password a través de un correo electrónico que se haya establecido u otro medio.

Una copia de seguridad es un proceso mediante el cual la información existente en cualquier dispositivo, se duplica en otro soporte. El motivo principal de llevar a cabo este proceso radica en lo siguiente: en caso de fallo del soporte que guarda los datos originales, estos se puedan recuperar estos a través de un segundo.

Por tanto, las copias de seguridad resultan muy útiles ante distintos escenarios. Como ejemplo, a la hora de recuperar los datos tras recibir un ciberataque, tras una eliminación accidental o tras una infección por un virus, entre otros casos.

Esto quiere decir que se deben realizar porque la pérdida de información o datos importantes supone, a la vez, desperdiciar horas de trabajo. Y esto desencadenaría pérdidas económicas. Herrero, E. G. (2022) comenta:

> Para saber qué datos se deben guardar, en primer lugar, habría que conocer la totalidad de los activos de información que existen y, seguidamente, clasificarlos. El objetivo principal de este proceso es tener registrado todo el software para conocer la periodicidad de llevar a cabo las copias de seguridad. A mayor número de activos, mayor debe ser la frecuencia con la que se hagan las copias. (párr.4)

En cuanto al almacenamiento, existen varios dispositivos los cuales se puede tener en cuenta a la hora de guardar las copias de seguridad. El soporte elegido depende de la cantidad de archivos, del sistema seleccionado y de la inversión económica que se desee realizar:

Las cintas magnéticas DAT/DDS/LTO son durante mucho tiempo una opción popular para el almacenamiento de copias de seguridad, especialmente para empresas con grandes volúmenes de datos. Su principal ventaja radica en su coste reducido y su capacidad para almacenar grandes cantidades de archivos. Además, tienen una vida útil notable, puede alcanzar hasta los 30 años si se almacenan y manipulan adecuadamente. Esta longevidad es esencial para las empresas que necesitan conservar registros y datos a largo plazo, proporcionando una forma segura y confiable de preservar información valiosa. Sin embargo, es crucial tener en cuenta que, aunque son duraderas, las cintas magnéticas necesitan condiciones de almacenamiento específicas para garantizar su integridad a lo largo del tiempo.

La opción de almacenamiento en la nube gana una popularidad significativa en los últimos años debido a su comodidad y accesibilidad. Consiste en guardar las copias de seguridad en servicios ofrecidos por terceros, como Dropbox, OneDrive y Google Drive. La ventaja clave de esta opción es la capacidad de acceder a los datos desde cualquier lugar con una conexión a Internet. Sin embargo, la seguridad es una preocupación principal al elegir el almacenamiento en la nube. Los usuarios deben cifrar todas sus copias de seguridad antes de cargarlas en la nube para proteger la privacidad y confidencialidad de los datos. Además, es importante considerar los costos a largo plazo, pues algunos servicios de almacenamiento en la nube pueden resultar caros para grandes volúmenes de datos.

Los discos ópticos, como los CD y DVD, son una opción adecuada para empresas que no necesitan proteger una gran cantidad de datos, ni realizar copias de seguridad con

frecuencia. Son ideales para almacenar datos importantes de forma segura y a largo plazo, pero su capacidad es limitada en comparación con otros dispositivos de almacenamiento, como los discos duros. Además, los discos ópticos son portátiles y fáciles de almacenar, lo cual los convierte en una opción conveniente para empresas con necesidades de almacenamiento modestas.

Los dispositivos externos, como las unidades USB y los discos duros externos, son prácticamente imprescindibles en entornos empresariales y domésticos. Ofrecen una gran facilidad para trasladar documentos y archivos de un lugar a otro, esto los convierte en herramientas versátiles para las copias de seguridad. Además, estos dispositivos suelen tener capacidades significativas de almacenamiento y son relativamente asequibles. La portabilidad y la capacidad de almacenamiento, hacen los dispositivos externos sean una opción popular para las personas quienes necesitan realizar copias de seguridad de datos importantes de manera regular. Sin embargo, es fundamental manejar estos dispositivos con cuidado y considerar medidas de seguridad adicionales para evitar pérdidas de datos debido a daños físicos o robo. Según IBM (2023) se comenta:

> Tape Library es una solución de alta densidad, altamente escalable y fácil de gestionar, diseñada para mantener los datos almacenados de forma segura a largo plazo, a la vez que ayuda a reducir los costos asociados con el espacio y las utilidades del centro de datos. (párr.1)

La copia de seguridad en local se refiere al proceso de crear una copia de seguridad del sistema, aplicaciones y datos en el mismo ordenador o, en dispositivos de almacenamiento conectados directamente a él. Aunque es una opción sencilla y conveniente tiene sus limitaciones. Por un lado, si el ordenador principal sufre un fallo grave o un ataque de malware, las copias de seguridad locales también podrían estar en riesgo. Por eso se recomienda combinar la copia de seguridad en local con otras opciones, como almacenamiento en la nube o dispositivos externos, para garantizar una protección completa y redundante de los datos. A pesar de estas limitaciones, las copias de seguridad locales siguen siendo valiosas para la recuperación rápida de datos en casos de pérdida o corrupción de archivos, siempre y cuando se realicen de forma regular y se almacenen en un lugar seguro.

Teniendo en cuenta todo esto, según Informaticos.co. (2023) se puede decir que existen cuatro tipos principales de copias de seguridad:

La copia de seguridad en espejo representa la forma más inmediata y continua para resguardar los datos. Este tipo de copia se realiza en tiempo real, significa que mientras

el usuario trabaja en su computadora, los archivos se copian automáticamente a otro medio de almacenamiento. Dicha técnica ofrece una protección casi instantánea contra la pérdida de datos, pues los archivos se duplican en el momento de su creación o modificación.

Sin embargo, aunque es efectiva para la recuperación inmediata, tiene sus limitaciones. Si se produce un error o una pérdida de datos inadvertida, los cambios no deseados también se van a replicar en la copia de seguridad en espejo. Por lo tanto, aunque es una forma rápida de preservar datos importantes, no reemplaza la necesidad de realizar copias de seguridad periódicas y más estructuradas para evitar pérdidas significativas en caso de fallos graves del sistema.

También se puede recurrir a una configuración RAID, según Fernández, Y. (2020) "es un método para combinar los discos duros como un matriz que se reconoce como una sola unidad por el sistema operativo. Dicho de forma sencilla, sería como configurar una unidad de almacenamiento formada por varios discos duros". (párr.4) Lo que hace esta configuración es enlazar los datos en varios discos duros, haciendo las operaciones de entrada y salida de datos estén mejor balanceadas, esto al final, acaba ayudando a tener un mejor rendimiento.

La copia de seguridad completa es el método más básico y ampliamente utilizado para respaldar datos. Como su nombre indica, este tipo de copia de seguridad implica duplicar todos los datos del sistema en otro medio de almacenamiento. Es una imagen completa y exacta de todos los archivos, programas y configuraciones presentes en el sistema en el momento de la copia.

Aunque es una estrategia sólida para preservar la integridad de los datos, también puede ser intensiva en tiempo y recursos, especialmente en sistemas con grandes volúmenes de datos. Sin embargo, la ventaja de las copias de seguridad completas radica en su capacidad para proporcionar una restauración rápida y sin complicaciones en caso de pérdida de datos importante. A menudo, las copias de seguridad completas se combinan con otros tipos de copias de seguridad, para optimizar la eficiencia y reducir el tiempo y el espacio requeridos para almacenar los datos de manera segura.

La copia de seguridad diferencial se centra en los datos que han cambiado desde la última copia de seguridad completa. A diferencia de la copia de seguridad en espejo, que se realiza en tiempo real, la diferencial se ejecuta en intervalos programados, generalmente diarios. En cada ejecución, se copia los archivos y datos modificados desde la última copia de seguridad completa, lo que reduce el tiempo y los recursos necesarios

en comparación con las copias de seguridad completas. Sin embargo, un aspecto importante por considerar es que, con el tiempo, las copias diferenciales pueden volverse considerablemente grandes. Esto, pues cada nueva copia diferencial se acumula con las anteriores, lo que puede resultar en un consumo significativo de espacio de almacenamiento. A pesar de esta desventaja, las copias de seguridad diferenciales ofrecen un equilibrio entre eficiencia y capacidad de recuperación, permitiendo restaurar los datos al estado en cual se encuentran en el momento de la última copia de seguridad completa.

La copia de seguridad incremental se basa en copiar únicamente los datos que han cambiado desde la última copia de seguridad, ya sea completa, diferencial o incremental. A diferencia de las copias de seguridad diferenciales, las incrementales solo se centran en los cambios desde la última copia, sin tener en cuenta las copias de seguridad anteriores.

Esto significa que las copias de seguridad incrementales tienden a ser más pequeñas en tamaño en comparación con las diferenciales a medida que pasa el tiempo. Sin embargo, durante el proceso de restauración, se requiere todas las copias de seguridad incrementales desde la última copia completa, para reconstruir los datos. Esto puede hacer el proceso de recuperación sea más complejo y llevar más tiempo en comparación con las diferencias. A pesar de ello, las copias de seguridad incrementales son eficientes en cuanto a espacio y son útiles para minimizar el uso de recursos de almacenamiento, especialmente en sistemas con cambios frecuentes, pero con limitaciones de capacidad de almacenamiento.

El cifrado de datos es un método de protección de datos, consiste en alterarlos hasta hacerlos ilegibles. Los datos pasan de ser texto sin formato a ser texto cifrado por medio de un método denominado algoritmo. Quien desee acceder a los datos cifrados debe descodificarlos primero con la clave de descifrado correcta.

El cifrado de datos aumenta la seguridad de sus datos confidenciales y su información personal, le ofrece protección y privacidad en un mundo en línea totalmente imprevisible.

Según Derek DeWitt. (2022). “El cifrado funciona pasando los datos originales (o texto plano) por un algoritmo (o cifra) que los convierte en texto cifrado. El nuevo texto resulta ilegible si no se utiliza la clave de descifrado adecuada para descodificarlo.” (párr.5)

Esto es igualmente cierto para los datos en reposo (almacenados en algún sitio, como un disco duro) y en movimiento (en transferencia electrónica de un lugar a otro, por ejemplo, a través de una red o de Internet).

Los algoritmos de cifrado emplean claves criptográficas (cadenas de caracteres) para transformar los datos en un sinsentido aparentemente aleatorio. Los algoritmos modernos descomponen los datos de texto plano en grupos llamados bloques y luego cifran cada bloque como una unidad. Por este motivo se les denomina cifradores de bloques.

Los algoritmos actuales son tan complejos que el texto plano puede terminar como un texto cifrado distinto cada vez que se aplican. Los datos solo se logran descodificar con la clave para esa sesión de cifrado específica.

La auditoría de seguridad como menciona DocuSign. (2021). “es una evaluación del nivel de madurez de la seguridad de una empresa, en la cual se analizan las políticas y procesos de seguridad establecidos por esta para revisar minuciosamente el grado de cumplimiento.” (párr.5). Además, existen medidas técnicas y organizativas determinadas para una mayor solidez.

Luego de obtener los resultados de esta, se detallan y almacenan para notificar a los responsables, con el fin de que elaboren medidas correctivas y preventivas de refuerzo y, de esta manera, logren sistemas más estables.

Un firewall o cortafuegos, Gómez, J. A. (2023) comenta:

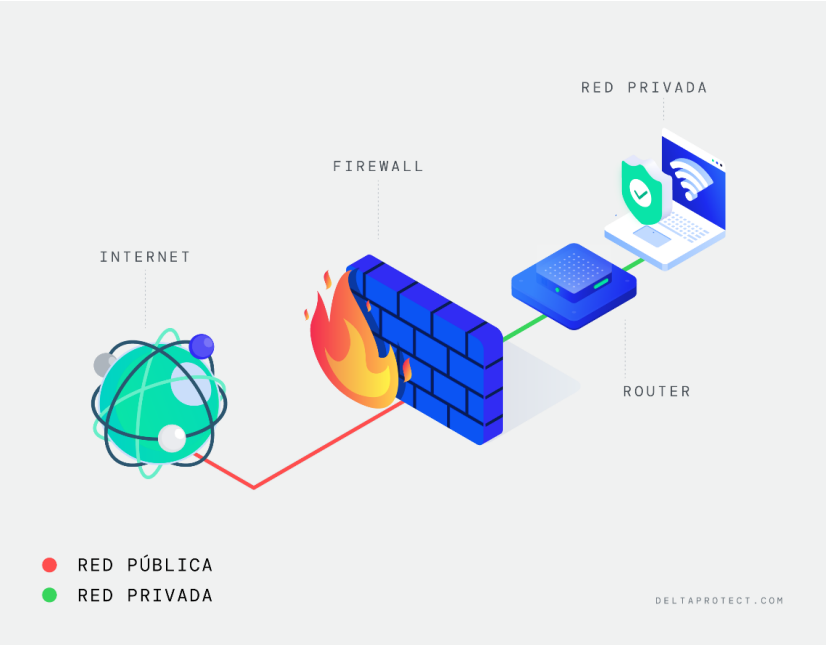
> es un elemento informático que controla el tráfico entrante y saliente de un dispositivo o una red privada con la finalidad de bloquear la entrada de datos que no cumplan con algunos criterios de seguridad. Estos criterios pueden ser adaptados a las necesidades particulares de cada individuo o empresa. (párr.1)

El firewall actúa literalmente como un muro el cual se construye en un punto entre el ordenador o red interna deseada de proteger y una red pública (es decir, el internet). Examina cada dato que intenta transitar de, y hacia la red interna, permitiendo su paso si cumple con los criterios ya establecidos y evitando su ingreso si no los cumple.

De esta manera, el firewall evita intrusiones de usuarios no autorizados y de data maliciosa capaces de poder dañar los sistemas o dispositivos conectados a una red de acceso local o LAN (del inglés local access network), para proteger datos personales o los datos de la empresa de algunos ataques provenientes de la red.

Ilustración 1

Firewall



Fuente: https://Firewall.png

Como se puede observar en la ilustración, la función principal de un firewall es proteger los dispositivos conectados a una red privada de accesos no autorizados y de información o solicitudes de entrada maliciosas. Para cumplir con esa función, el firewall debe supervisar y filtrar todos los datos e intentos de acceso para dividirlos en dos grupos: aquellos que cumplen con los criterios de seguridad establecidos y se les permite el paso, y aquellos que no los cumplen y son bloqueados.

Así, actúa como primera línea de defensa y en algunos casos impide el acceso de usuarios no autorizados, en otros detecta el robo o la exfiltración de información y la presencia de algunos tipos de malware mediante el análisis de red, entre otras amenazas cibernéticas.

Según Gómez, J. A. (2023) estas son algunas de las funciones o elementos que un firewall debe cumplir:

- Supervisar la comunicación saliente o entrante de los equipos conectados a una misma red o al internet.
- Algunos fabricantes de Firewall permiten advertir y evitar el acceso de usuarios no autorizados a la red interna.
- Bloquear el tráfico de red asociado a aplicaciones específicas que parezcan sospechosas o maliciosas.

- Advertir los intentos de conexión que ocurren desde dispositivos desconocidos.
- Evitar que ingrese desde la red algunos tipos de malware.
- Adaptarse a los cambios y progresos que ocurren en los ataques cibernéticos. (párr.6)

Según lo menciona IBM. (2023). “Un sistema de detección de intrusiones (IDS) es una herramienta de seguridad de red que supervisa el tráfico y los dispositivos de la red en busca de actividades maliciosas conocidas, actividades sospechosas o infracciones de las políticas de seguridad.” (párr.1)

Un IDS puede ayudar a acelerar y automatizar la detección de amenazas en la red alertando a los administradores de seguridad sobre amenazas conocidas o potenciales, también enviando alertas a una herramienta de seguridad centralizada, como un sistema de gestión de eventos e información de seguridad (SIEM), donde pueden combinarse con datos de otras fuentes para ayudar a los equipos de seguridad a identificar y responder a ciberamenazas que podrían escapar a otras medidas de seguridad.

Los IDS también pueden apoyar los esfuerzos de cumplimiento de la normativa. Ciertas normativas, como la norma de seguridad de datos del sector de las tarjetas de pago (PCI-DSS, por sus siglas en inglés), exigen las organizaciones apliquen medidas de detección de intrusiones.

Las empresas contables deben cumplir con las regulaciones y estándares de seguridad de la información aplicables en su país o industria, como el Reglamento General de Protección de Datos (RGPD) en la Unión Europea.

Otra manera para que el sistema contable sea seguro: se debe capacitar al personal de la empresa sobre la seguridad del sistema, es importante concientizar y capacitar al personal sobre la importancia de la seguridad de la información. Esto puede incluir la sensibilización sobre los riesgos de seguridad, la identificación de ataques de phishing y el uso adecuado de contraseñas.

El phishing se refiere al envío de correos electrónicos, los cuales tienen la apariencia de proceder de fuentes de confianza, pero en realidad pretenden manipular al receptor para robar información confidencial. Por eso siempre es recomendable acceder a las páginas web escribiendo la dirección directamente en el navegador. Panda Security. (s. f.) comenta:

La mayoría de los ataques de phishing comienzan con la recepción de un correo electrónico o un mensaje directo en el que el remitente se hace pasar por un banco, una

> empresa u otra organización real, con el fin de engañar al destinatario. Este correo electrónico incluye enlaces a un sitio web preparado por los criminales -que imita al de la empresa legítima- y en el que se invita a la víctima a introducir sus datos personales. (párr.3)

En este sentido existe una vinculación entre el spam y el phishing, pues los correos electrónicos fraudulentos suelen enviarse de forma masiva para multiplicar el número de víctimas potenciales de los hackers. De hecho, si bien el e-mail continúa siendo el medio más utilizado por los ciberdelincuentes para este tipo de fraudes, el phishing puede utilizar otros medios de comunicación, además son frecuentes los intentos vía SMS (a veces llamados smishing), VoIP (vishing) o los mensajes instantáneos en redes sociales.

Así los criminales se valen de ciertos trucos de ingeniería social para crear alarma en los receptores de los mensajes, con indicaciones de urgencia, alarma y diferentes llamadas a la acción. La idea es que el usuario actúe de inmediato ante el estímulo y no se detenga a analizar los riesgos de su acción.

La seguridad de un sistema contable es un requisito fundamental para cualquier organización que gestione información financiera. La norma ISO 27001 proporciona un marco para proteger la información financiera de una organización contra una serie de amenazas, como el acceso no autorizado, la modificación o destrucción de datos y, la divulgación de información confidencial. Akamai. (2023) comenta:

> La ISO/IEC 27001 es una norma de seguridad de la información reconocida internacionalmente, desarrollada por el organismo de certificación Organización Internacional de Normalización (ISO) y la CEI (Comisión Electrotécnica Internacional). La norma ISO 27001 ha pasado por varias versiones, incluida la norma ISO 27001:2013; la última versión es la norma ISO/IEC 27001:2022. (párr.1)

La norma ISO 27001 proporciona directrices y un marco, con requisitos para "establecer, implementar, mantener y mejorar continuamente" un sistema de gestión de la seguridad de la información (ISMS). La norma ISO 27001 comprende 93 controles de gestión de riesgos, pero no todos son necesarios para cumplir con la norma ISO 27001; en su lugar, el cumplimiento de la norma ISO 27001 consiste en comprender el nivel de riesgo de su organización y decidir cuáles de los 93 controles son los más adecuados para mitigar ese riesgo para los activos de información.

La norma ISO 27001 requiere el establecimiento de un marco de ISMS ISO 27001 para recopilar políticas y procedimientos que protejan los datos confidenciales de una organización, incluida la propiedad intelectual. Este marco se basa en los procesos, las

personas, la tecnología y los procedimientos necesarios para los controles de seguridad de la información, con el fin de proteger los sistemas y los dispositivos, así como los datos de accesos no autorizados que pueden provocar el uso indebido, la exposición, la interrupción, la modificación o la destrucción de los datos. Además, las políticas y los procedimientos de ISMS ayudan a reducir el riesgo de los datos frente a ciberataques y amenazas internas mediante la evaluación de riesgos. Un ISMS también ayuda a cumplir con las normativas de protección de datos y privacidad, como el Reglamento General de Protección de Datos (RGPD), por cuanto ayuda a garantizar la integridad, confidencialidad y disponibilidad de los datos.

Según menciona Akamai. (2023) "La norma ISO 27001 consta de controles que abarcan las áreas de organización, personal, física y tecnológica. Estos sectores corren el riesgo de sufrir ciber amenazas centradas en las personas que explotan el acceso a sistemas y servicios críticos." (párr.5)

Una estrategia fundamental dentro de los objetivos de control de la norma ISO 27001 es el de la seguridad Zero Trust. Los controles incluyen:

Control de acceso, para establecer controles de acceso físicos y lógicos a la información y otros activos asociados.

Derechos de acceso con privilegios, para garantizar el acceso de "privilegio mínimo". Segregación de redes, como parte de una estrategia de seguridad Zero Trust. Estos controles ayudan a una organización a establecer un entorno Zero Trust. Akamai. (2023) comenta lo siguiente:

> La seguridad de los datos es una ventaja competitiva reconocida. La obtención de la certificación ISO 27001 ayuda a las organizaciones a demostrar a los clientes y otras partes interesadas que su empresa se toma en serio la seguridad de la información y cuenta con una gestión de continuidad de las actividades empresariales. El cumplimiento de la norma ISO 27001 significa que ha creado un entorno seguro, basado en un ISMS, que mitiga los riesgos de seguridad de los datos y ayuda a minimizar los riesgos para las empresas con las que hace negocios. (párr.13)

Al pasar por el proceso, implementar un conjunto de controles para gestionar las amenazas de seguridad de la información y mejorar la gestión de incidentes, su organización realiza un análisis de brechas de seguridad de los datos y tiene un menor riesgo de ciberataques y exposición accidental de los datos. Esto se traduce en menos filtraciones de datos y una menor probabilidad de multas y otras sanciones por incumplimiento de las normativas.

Los controles y el marco de la ISO 27001 se asignan a otras normativas de protección de datos, como el RGPD y el CSF (marco de ciberseguridad) del NIST. Por lo tanto, contar con la certificación ISO 27001 ayuda a cumplir con estas otras normativas de protección de datos.

A continuación, se presenta algunos ejemplos de controles específicos, los cuales las organizaciones pueden implementar con el fin de cumplir con los requisitos de la norma ISO 27001 para la seguridad de un sistema contable:

La autenticación multifactor es una tecnología de seguridad, requiere múltiples métodos de autenticación de categorías independientes de credenciales con el propósito de verificar la identidad de un usuario para un inicio de sesión u otra transacción. La autenticación multifactor combina dos o más credenciales independientes: lo que el usuario sabe, como una contraseña; lo que tiene el usuario, como un token de seguridad; y qué es el usuario, mediante el uso de métodos de verificación biométrica.

El objetivo de MFA es crear una defensa en capas y esta dificulte que una persona no autorizada acceda a un objetivo, como una ubicación física, un dispositivo informático, una red o una base de datos. Si un factor se ve comprometido o roto, el atacante todavía tiene al menos una o más barreras que romper antes de entrar con éxito en el objetivo.
Cloudflare. (2023) comenta:

> La encriptación es una forma de codificar los datos para que solo las partes autorizadas puedan entender la información. En términos técnicos, es el proceso de convertir un texto plano legible para seres humanos en un texto incomprensible, también conocido como texto encriptado. Si usamos términos más sencillos, la encriptación coge datos legibles y los altera para que parezcan aleatorios. La encriptación requiere el uso de una clave criptográfica: un conjunto de valores matemáticos pactados tanto por el emisor como por el receptor de un mensaje encriptado. (párr.1)

La encriptación es un proceso matemático, altera los datos al usar un algoritmo de encriptación y una clave. Imagine que Alicia envía el mensaje "Hola" a Bob, pero sustituye cada letra de su mensaje por la letra que le sigue dos lugares más adelante en el alfabeto. En lugar de "Hola," su mensaje ahora dice "Jgnnq". Afortunadamente, Bob sabe que la clave es "2" y puede descifrar su mensaje a "Hola."

Ilustración 2

Cifrado

Fuente: https://encryption-example.svg

Aunque los datos encriptados parezcan aleatorios, la encriptación procede de una forma lógica y predecible, lo anterior permite una parte reciba los datos encriptados y posea la clave adecuada pueda desencriptarlos y convertirlos de nuevo en texto plano. Una encriptación verdaderamente segura usa claves lo suficientemente complejas como para que sea muy improbable un tercero pueda desencriptar o descifrar el texto encriptado con fuerza bruta — es decir, adivinando la clave. Los datos pueden estar encriptados "en reposo," cuando están almacenados, o "en tránsito," mientras se están transmitiendo a otro lugar.

Una clave criptográfica es una cadena de caracteres, se utiliza en un algoritmo de encriptación para alterar los datos de forma que parezcan aleatorios. Como sucede con una llave física, esta bloquea (encripta) los datos para así, solo quien tenga la llave correcta pueda abrirlos (desencriptarlos).

El control de acceso basado en roles (RBAC) es un mecanismo de control de acceso, este define los roles y privilegios para determinar si a un usuario se le debe dar acceso a un recurso. Los roles se definen en función de características como la ubicación, el departamento, la antigüedad o las funciones de un usuario. Los permisos se asignan según el acceso (lo que el usuario puede ver), las operaciones (lo que el usuario puede hacer) y las sesiones (cuánto tiempo puede hacerlo el usuario).

También, es necesario desarrollar políticas y procedimientos de seguridad para guiar a los empleados en la protección de la información del sistema contable. Villanueva, A. (2021) comenta al respecto:

Contar con políticas de seguridad es imprescindible para poder garantizar la integridad de los sistemas, pues además de garantizar la seguridad, establece un comportamiento y controles necesarios para aplicar las estrategias de la empresa. También ayuda a determinar cómo prevenir y responder a amenazas a la integridad, disponibilidad y confidencialidad de la información y activos críticos, identificando las responsabilidades, derechos y deberes de los trabajadores. (párr.1)

CAPÍTULO III: MARCO METODOLÓGICO

En este capítulo se presenta los diferentes enfoques y tipos de investigación más comunes y utilizados, para así brindar al lector una idea más completa de las diferentes formas por abordar en esta investigación

Enfoques de Investigación

. Enfoque Cuantitativo: En este enfoque se recopila los datos numéricos mediante encuestas estructuradas, cuestionarios, mediciones y otras técnicas estandarizadas. Los datos se analizan utilizando métodos estadísticos como promedio, desviación estándar y pruebas de significancia. El análisis estadístico ayuda a identificar patrones, correlaciones y relaciones causales. En este enfoque, la objetividad es crucial. Los resultados buscan ser objetivos, reproducibles y generalizables a la población en general. El propósito es controlar las variables para evitar sesgos. Los instrumentos de medición están estandarizados para garantizar respuestas consistentes.

Enfoque Cualitativo: En este enfoque se obtiene los datos no numéricos a través de entrevistas, observaciones, grupos focales y análisis de documentos. El objetivo es comprender el contexto, la perspectiva y el significado. Los datos cualitativos se analizan interpretativamente, los patrones y temas emergen a través del análisis, permitiendo comprender fenómenos complejos y contextuales. Este enfoque busca profundidad y comprensión del por qué y el cómo de comportamientos y experiencias. Los datos cualitativos suelen venir acompañados de citas y ejemplos los cuales respaldan las afirmaciones.

Enfoque Mixto: En este enfoque se combina datos cuantitativos y cualitativos en una sola investigación. La integración puede ser simultánea (se recopila datos cuantitativos y cualitativos simultáneamente) o secuencial (una fase de investigación sigue a otra). Los métodos cualitativos y cuantitativos están diseñados para complementarse y proporcionar una visión más completa del problema de investigación.

Enfoque Cuantitativo:

Este método es adecuado cuando se desea recopilar datos numéricos y realizar análisis estadísticos para obtener resultados objetivos y generales. Los métodos cuantitativos pueden ser la mejor opción cuando el objetivo principal es medir variables, establecer relaciones o hacer comparaciones cuantitativas.

Se basa en la idea de que los datos numéricos son los puntos encargados de brindar una base sólida para el análisis e interpretación de la variable o fenómeno en cuestión. El objetivo de este método es obtener mediciones precisas y confiables, mediante el uso de

métodos estandarizados como cuestionarios, escalas de medición o registros. Recopile datos y realice análisis sistemáticos para sacar conclusiones significativas.

Enfoque de Investigación Seleccionado

Se elige el enfoque cuantitativo, pues la seguridad en los sistemas de contables proporciona una base sólida para la toma de decisiones y la mejora continua de la seguridad, la cual le permite analizar datos numéricos para comprender las tasas de incidentes, la eficacia de las medidas de seguridad, las tendencias de los ataques cibernéticos de seguridad y este método es útil para recopilar datos cuantitativos sobre cuestiones como la frecuencia de los incidentes de seguridad, la eficacia de las medidas de seguridad o las tendencias de los ciberataques. Es muy bueno para proporcionar datos numéricos que pueden compararse y analizarse estadísticamente.

A través del análisis estadístico, ofrece datos numéricos precisos y fácilmente comparables. Puede hacer esto para encontrar patrones y correlaciones en los datos, que pueden brindarle información importante sobre amenazas y vulnerabilidades. Ayuda a los líderes a tomar decisiones informadas sobre inversiones en seguridad y cambios de políticas al proporcionar datos concretos.

Tipos de Investigación

Investigación descriptiva: Como su título lo indica, se encarga de describir las características de la realidad por estudiar con el fin de comprenderla de manera más exacta. En este tipo de investigación, los resultados no tienen una valoración cualitativa, solo se utilizan para entender la naturaleza del fenómeno.

Investigación exploratoria: Se utiliza cuando el objetivo es hacer una primera aproximación a un asunto desconocido o sobre el cual no se ha investigado lo suficiente. Esto permite decidir si efectivamente se puede realizar investigaciones posteriores y con mayor profundidad. Como este método parte del análisis de fenómenos poco estudiados, no se apoya tanto en la teoría, sino en la recolección de datos que permitan detectar patrones para dar explicación a dichos fenómenos.

Investigación explicativa: Es el tipo de investigación más común y se encarga de establecer relaciones de causa y efecto que permitan hacer generalizaciones y puedan extenderse a realidades similares. Es un estudio muy útil para verificar teorías.

Investigación descriptiva

El utilizar una investigación descriptiva brinda una descripción más precisa y profunda del tema investigado, el objetivo principal es recopilar datos para poder comprender con

mayor precisión el tema en estudio. Este tipo de investigación utiliza una variedad de técnicas aplicadas para recopilar información, incluidas encuestas, observaciones, entrevistas y análisis de documentos. Cuando se adquiere esta información, se examina y organiza para su presentación con el fin de proporcionar una imagen más clara y con más cualidades que llevan a conclusiones correctas.

Al ofrecer una mayor cantidad de datos para próximos estudios o investigaciones, este tipo de estudio es muy beneficioso en una variedad de campos.

Tipo de Investigación Seleccionado

Debido a ser el objetivo principal obtener información precisa de la evaluación de los apartados de la investigación, se decide utilizar un tipo descriptivo para recopilar datos a través de una encuesta de calificación y, analizarlos estadísticamente para una presentación adecuada.

Utilizando una escala de calificación del 1 al 5, se puede cuantificar las respuestas y obtener los porcentajes requeridos, permitiendo obtener calificaciones en relación con cada apartado de la investigación. Este método permite recopilar información directamente de los empleados con base en su experiencia.

Fuentes de información

Las fuentes de información son esenciales para la investigación y el aprendizaje, en tanto proporcionan una amplia gama de conocimientos en diversos campos. Se puede considerar como fuentes libros, escritos académicos, sitios web confiables o expertos en la materia quienes brinden información y opiniones reflexivas. La utilización de fuentes confiables permite verificar los datos compartidos y tomar decisiones defendibles tanto en la vida personal como profesional.

Fuentes de información primaria: Son aquellas que dan una información nueva u original y no ha sido recogida o recopilada de antemano. Principalmente se trata de la información incluida en publicaciones más serias o monografías (libros y revistas) y sus partes, como los capítulos, artículos y otros. De ellas se obtiene directamente la información.

Fuentes de información secundaria: Son aquellas que, por el contrario, no tienen como objetivo principal ofrecer información, sino indicar cuál fuente o documento la puede proporcionar, es decir, facilitan la localización e identificación de los documentos. No contienen información acabada, siempre remiten a documentos primarios. Son bibliografías, catálogos, bases de datos, entre otras.

Fuentes de información terciarias: Son recursos donde se recopila y organiza información proveniente de fuentes secundarias. Estas guías, ya sean virtuales o físicas, son valiosas herramientas para estudiantes, investigadores y profesionales, pues proporcionan una visión general y estructurada de un campo específico del conocimiento. Las fuentes terciarias incluyen enciclopedias, diccionarios especializados, catálogos de bibliotecas y directorios académicos.

Variables

Variables operacionales: Desempeñan un papel crucial en la investigación al ser tangibles y cuantificables, proporcionan medidas exactas que demuestran un proceso de manera precisa. Estas variables destacan por su capacidad de definir con precisión la presencia y cantidad de un fenómeno, aportando a los investigadores datos precisos y concretos para su análisis.

Variables instrumentales: Se utilizan como medidas precisas para representar una variable particular. Estas mediciones ofrecen un punto de comparación estándar el cual permite comparar diversas circunstancias o contextos de manera significativa. Son cruciales para la investigación científica y social, porque crean un marco consistente para la evaluación y el análisis. Lo anterior facilita la interpretación precisa de los datos recopilados.

Variables conceptuales: Estas variables presentan un desafío único para los investigadores, pues no tienen una forma definida de ser medidas u observadas directamente. Representan ideas o conceptos abstractos imprecisamente cuantificables.

Tabla 2

Unidad de análisis

Objetivo	Variable	Variable conceptual	Variable Operacional	Variable Instrumental
Crear la política de restricción de navegación a internet de acuerdo con la norma ISO/IEC 27001.	Política de restricción	Según Alonso, C. (2023) “El propósito de una política de uso de Internet es definir lo que está permitido o no a	Encuesta Entrevista	Guía de encuesta Guía de entrevista

		la hora de utilizar la red.” (párr.1)		
Construir el procedimiento de las medidas para proteger y controlar los dispositivos que acceden a la información de acuerdo con la norma ISO/IEC 27001.	Medidas de protección	Según PowerData (s. f.) “se refiere a medidas de protección de la privacidad digital que se aplican para evitar el acceso no autorizado a los datos.” (párr.1)	Encuesta Entrevista	Guía de encuesta Guía de entrevista
Construir el procedimiento de seguridad de usuario para el control de acceso a sistema y aplicaciones de acuerdo con la norma ISO/IEC 27001.	Procedimiento de seguridad	Según Microsoft (2023) “el control de acceso es un elemento esencial de la seguridad que determina quién tiene permiso para tener acceso a determinados datos, aplicaciones y recursos y en qué circunstancias.” (párr.1)	Encuesta Entrevista	Guía de encuesta Guía de entrevista
Analizar la protección de los datos y la información, de	Protección de datos	Según Kim Hefner (2021) “la protección de datos es el	Encuesta Entrevista	Guía de encuesta Guía de entrevista

acuerdo con la norma ISO/IEC 27001		proceso de salvaguardar información importante contra corrupción, filtraciones, pérdida o compromiso de los datos.” (párr.1)		

Fuente: Elaboración Propia

Población

Es el conjunto o colección de objetos al cual está referido un estudio estadístico. El vocablo suena a personas, pero una población estadística puede estar constituida por cualquier tipo de elemento, es decir, una población puede estar constituida por personas, pero también por objetos de cualquier tipo de naturaleza.

Muestra

Cualquier subconjunto de una población. Cuando los elementos que componen la muestra están elegidos aleatoriamente y todos los elementos tienen igual probabilidad de ser elegidos, se dice tratarse de una muestra aleatoria simple. Por norma general, en un estudio estadístico hay muchos condicionantes de tipo económico, físico, o de otro tipo que impiden trabajar con todos los elementos de la población, por tanto, se suele recurrir a muestras representativas de la población. Para calcular la muestra se utiliza la siguiente fórmula:

Ilustración 3

Fórmula cálculo de muestra

$$n = \frac{K^2 Npq}{e^2(N-1) + K^2 pq}$$

Fuente: Elaboración propia

n= tamaño de la muestra.

N= tamaño de la población.

K= nivel de confianza.

p= proporción esperada.

q=probabilidad de fracaso.

e= precisión (margen de error).

Ilustración 4

Cálculo de muestra

$$n= \frac{1{,}645^2 * 21 * 0{,}50 * 0{,}50}{0{,}05^2 * (21 - 1) + 1{,}645^2 * 0{,}50 * 0{,}50}$$

$$n= 19{,}55472682$$

Fuente: Elaboración propia

Instrumento Utilizado para la Recolección de Datos

Respecto de la recolección de datos para los trabajadores de la empresa Landergren Consulting Group (LCG), se propone utilizar como instrumento para ello una encuesta, con base en el criterio de los empleados. Este método permite recopilar información de manera eficiente tomando en cuenta la cantidad de colaboradores con quienes cuenta la empresa. El instrumento consiste en un cuestionario estructurado con escalas de medición, donde cada participante asigna un puntaje a diferentes afirmaciones relacionadas con las variables de interés. Se utiliza una escala de múltiples opciones (de 1 a 5) para así, los trabajadores indiquen su criterio con cada afirmación, se realiza las encuestas vía web a través de las plataformas WhatsApp o Gmail, pues es muy sencillo ingresar a estas herramientas ampliamente utilizadas en el entorno laboral y ofrecen la posibilidad de enviar las encuestas de manera eficiente, sin necesidad de trasladarse hacia donde está la persona para poder encuestarla. Además, el formato digital facilita la recopilación y análisis de los datos, permite una respuesta rápida y confidencial por parte de los participantes. También se realiza una entrevista para reforzar y obtener resultados más precisos en cada respuesta de las preguntas proporcionadas

Al utilizar la calificación en las respuestas de la encuesta y entrevista se permite obtener datos cuantitativos, esto facilita el análisis estadístico posterior. Esos puntajes

reflejan la percepción de los trabajadores en cuanto a su criterio y conformidad de los sistemas utilizados a diario, gracias a estas respuestas se puede identificar los puntos de mejora y es posible realizar una investigación más completa.

CAPITULO IV: ANÁLISIS DE RESULTADOS

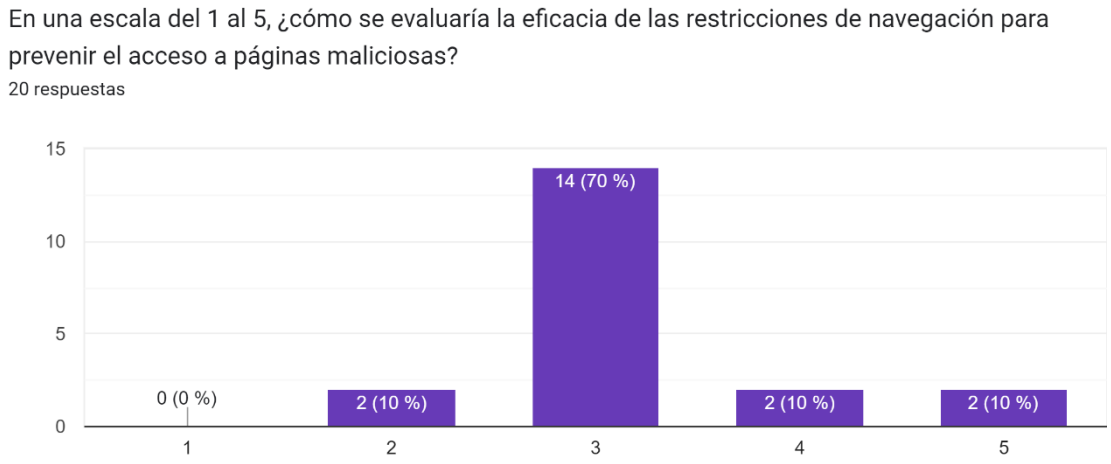
Encuesta

Se realiza una encuesta minuciosa a los empleados de la organización para determinar qué tan efectivas son las políticas y los protocolos aplicados hasta la fecha. Se pretende alcanzar una comprensión exhaustiva respecto de cómo los empleados sienten e interactúan con ciertos aspectos clave relacionados con el trabajo como son: las políticas de restricción de navegación, el control de acceso y criptografía, la gestión de credenciales y permisos, la seguridad de usuarios, la red, así como el control y prevención de correos electrónicos.

Se obtiene un análisis que permite evaluar el estado actual de seguridad informática en la empresa, identificando los éxitos alcanzados y las áreas donde se puede hacer mejoras. Al examinar las respuestas del entrevistado, se da énfasis en los puntos fuertes que contribuyen con la seguridad y también se identifica cualquier posible debilidad con necesidad de una pronta solución.

Ilustración 5

Gráfico donde se representa las respuestas a la pregunta No. 1



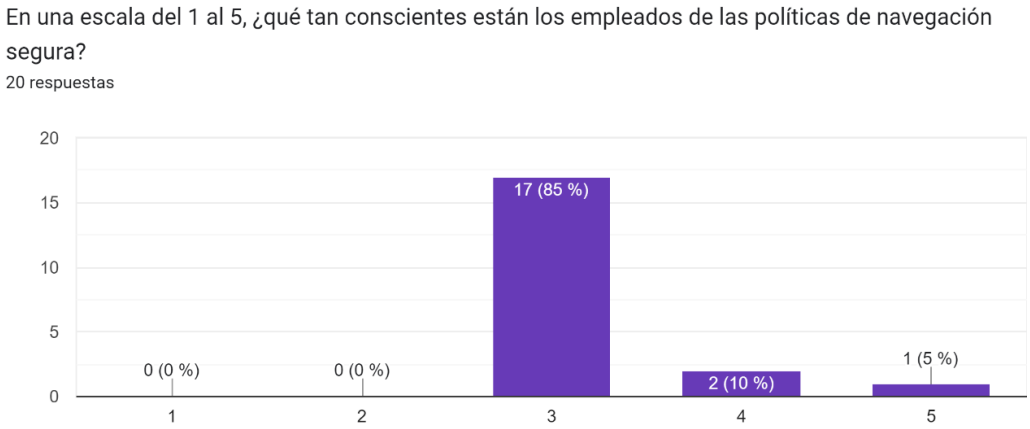
Fuente: Elaboración Propia

Se observa, con respecto de la eficacia de las restricciones de navegación para prevenir el acceso a páginas maliciosas, un 10% de los encuestados responde son malas, mientras un 70% indica son regulares. Un 10% indica son buenas y un 10% indica son muy buenas. En general se percibe: la mayoría de los encuestados opina que la eficacia de las

restricciones de navegación para prevenir el acceso a páginas maliciosas, no es la adecuada.

Ilustración 6

Gráfico donde se representa las respuestas a la pregunta No. 2

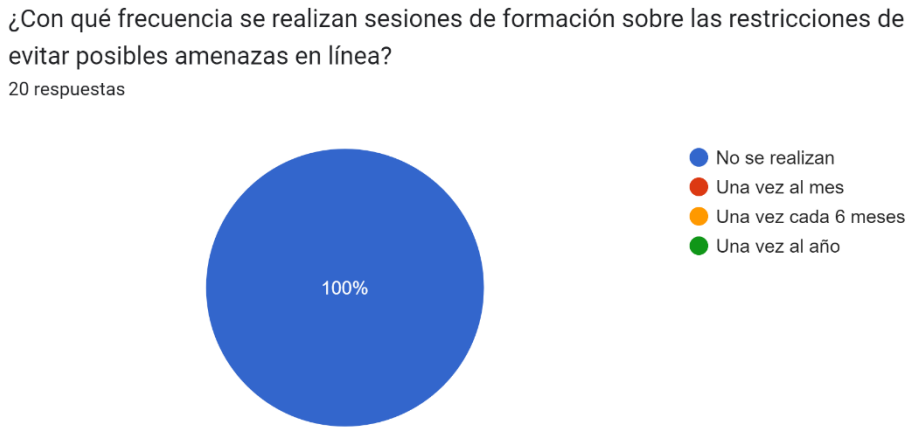


Fuente: Elaboración Propia

Se observa en cuanto a la conciencia de los empleados sobre las políticas de navegación por internet, un 85% de los encuestados la considera regular, un 10% manifiesta estar consciente y un 5% afirma estar muy consciente. Estos resultados sugieren que la mayoría de los participantes perciben la conciencia de los empleados sobre las políticas de navegación como insuficiente.

Ilustración 7

Gráfico donde se representa las respuestas a la pregunta No. 3

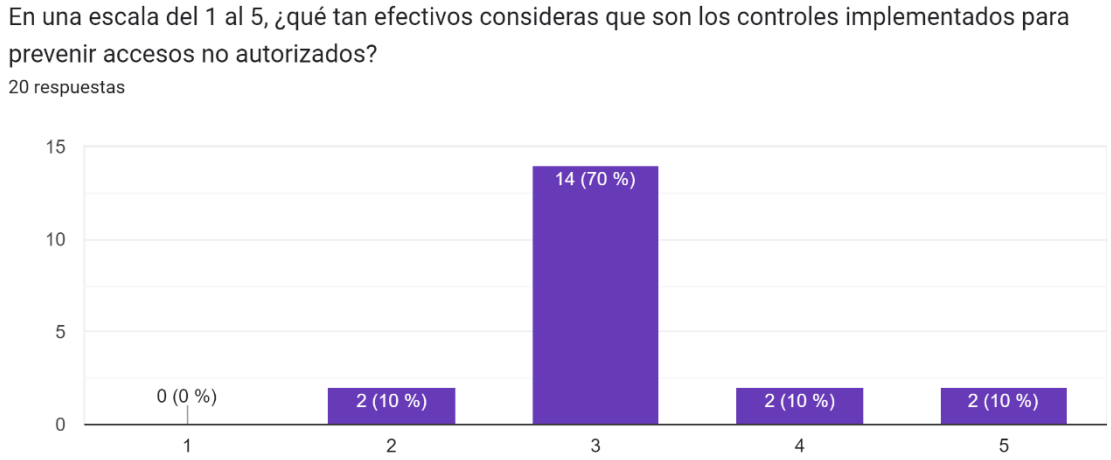


Fuente: Elaboración Propia

Se evidencia la ausencia de sesiones de formación relacionadas con las restricciones de navegación para prevenir posibles amenazas en línea, pues el 100% de los encuestados indica no se lleva a cabo tales sesiones. La falta de formación podría representar un riesgo potencial para la seguridad informática dentro del entorno evaluado.

Ilustración 8

Gráfico donde se representa las respuestas a la pregunta No. 4

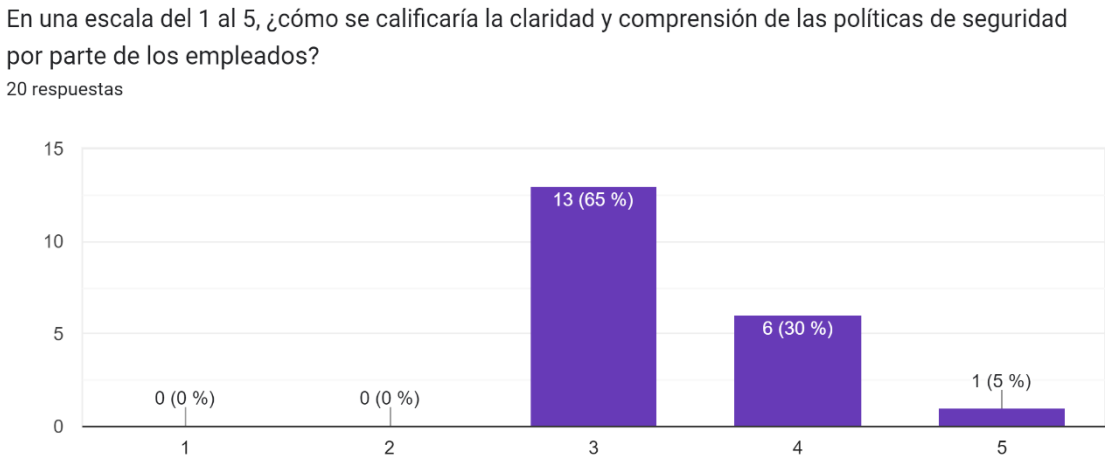


Fuente: Elaboración Propia

Se observa: con respecto de la valoración de los controles implementados para prevenir accesos no autorizados, los empleados expresan diversas opiniones. Un 10% de los encuestados considera dichos controles son malos, mientras un 70% los califica como regulares. Por otro lado, un 10% opina son buenos, y otro 10% los evalúa como muy buenos. En conjunto, estos resultados indican hay una diversidad de percepciones entre los empleados, pero la mayoría coincide en que los controles implementados para prevenir accesos no autorizados no alcanzan un nivel óptimo de eficacia.

Ilustración 9

Gráfico donde se representa las respuestas a la pregunta No. 5

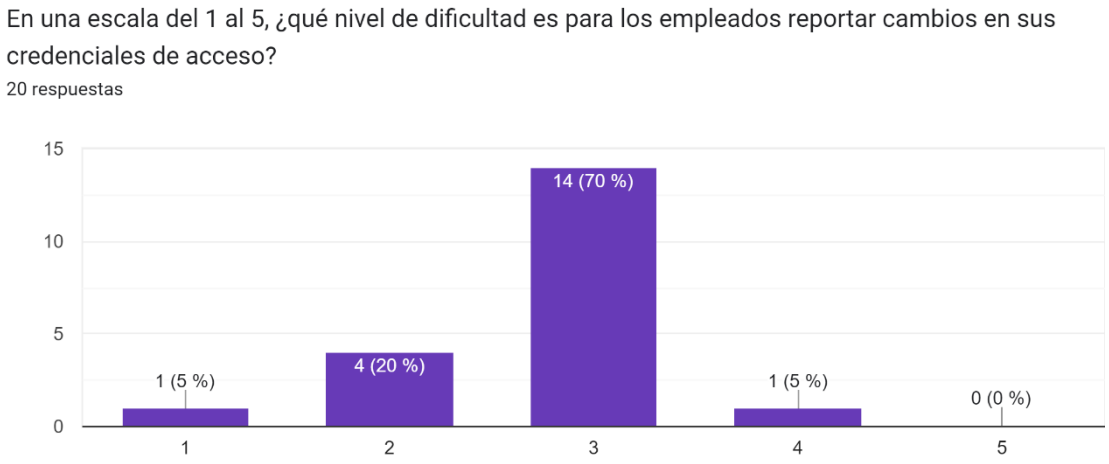


Fuente: Elaboración Propia

Se observa: los empleados califican la claridad y comprensión de las políticas de seguridad, un 65% las considera regulares, un 30% las percibe como buenas y un 5% las valora como muy buenas. Estos resultados sugieren, aunque hay una proporción significativa que ve las políticas como aceptables, aún existe un margen para mejorar la claridad y la comprensión de las políticas de seguridad.

Ilustración 10

Gráfico donde se representa las respuestas a la pregunta No. 6

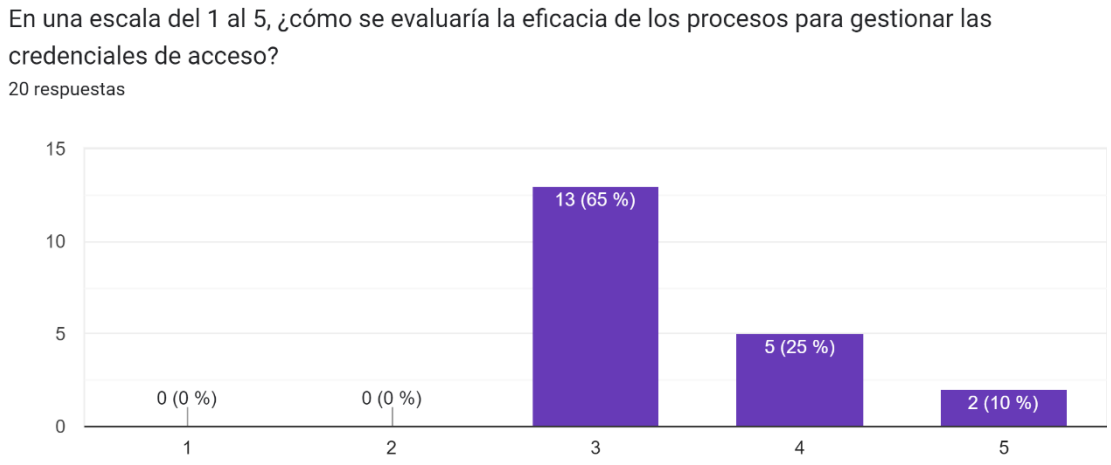


Fuente: Elaboración Propia

Se observa el nivel de dificultad para los empleados para reportar cambios en sus credenciales de acceso, un 5% considera es muy fácil, mientras un 20% lo percibe como fácil. La mayoría, con un 70%, lo califica como regular, indicando posiblemente una experiencia que podría mejorarse. Por otro lado, un 5% de los encuestados encuentra difícil realizar dicho reporte. Estos resultados indican lo siguiente: aunque hay una variedad de percepciones, existe una proporción importante de empleados quienes consideran la tarea de reportar cambios en las credenciales como un proceso posible de mejorar.

Ilustración 11

Gráfico donde se representa las respuestas a la pregunta No. 7

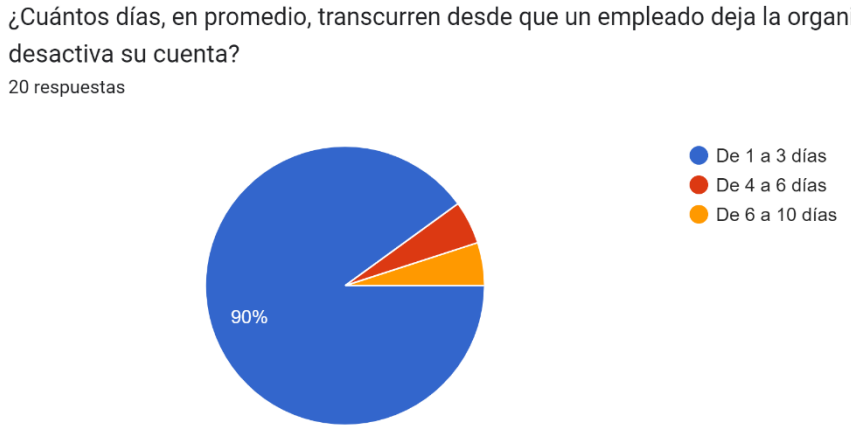


Fuente: Elaboración Propia

Se observa la percepción de los empleados respecto de la eficacia de los procesos para gestionar las credenciales de acceso. Un 65% de los encuestados la califica como regular, indican posiblemente áreas donde se podría mejorar la eficiencia y la experiencia del usuario. Por otro lado, un 25% la considera eficaz, señalan un nivel de satisfacción significativo. Un 10% la evalúa como muy eficaz. En general se percibe que la mayoría de los encuestados opina no es adecuada la eficacia de los procesos para gestionar las credenciales de acceso.

Ilustración 12

Gráfico donde se representa las respuestas a la pregunta No. 8

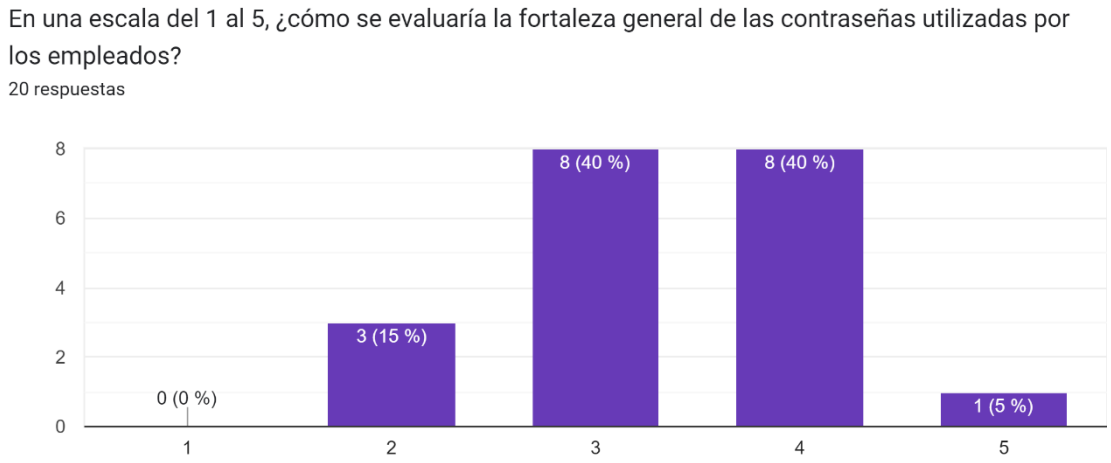


Fuente: Elaboración Propia

Se observa la percepción de los empleados con respecto del tiempo necesario para desactivar la cuenta de un trabajador. El 90% de los encuestados indica este proceso suele llevar de uno a tres días, lo cual sugiere una eficiencia general en la gestión de la desactivación de cuentas dentro de ese rango de tiempo. Por otro lado, el 5% de los votos señala el proceso toma de cuatro a seis días y, otro 5% indica puede extenderse de seis a diez días. Estos resultados indican que la gran mayoría de los empleados percibe el tiempo de desactivación de cuentas es razonablemente rápido, pero existe una minoría que experimenta plazos más largos.

Ilustración 13

Gráfico donde se representa las respuestas a la pregunta No. 9

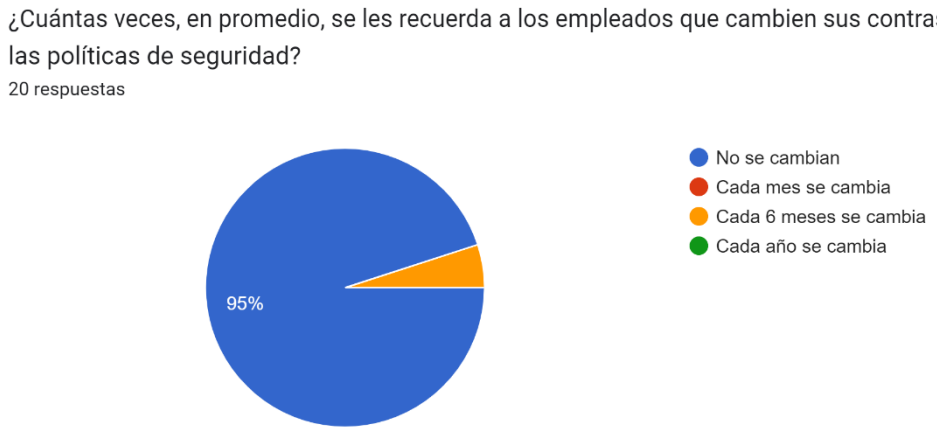


Fuente: Elaboración Propia

Se observa la evaluación de los empleados con respecto del nivel de fortaleza de las contraseñas. Un 15% considera es malo, indicando posiblemente áreas de debilidad en las prácticas de creación y gestión de contraseñas. Por otro lado, un 40% califica este nivel como regular, esto sugiere la existencia de una percepción acerca de que hay margen para mejorar la seguridad de las contraseñas. Un 40% lo valora como bueno, indicando un nivel satisfactorio de fortaleza en la mayoría de las contraseñas. Además, un 5% lo clasifica como muy bueno, lo cual sugiere hay una pequeña parte de empleados quienes perciben altos estándares de seguridad en las contraseñas utilizadas.

Ilustración 14

Gráfico donde se representa las respuestas a la pregunta No. 10

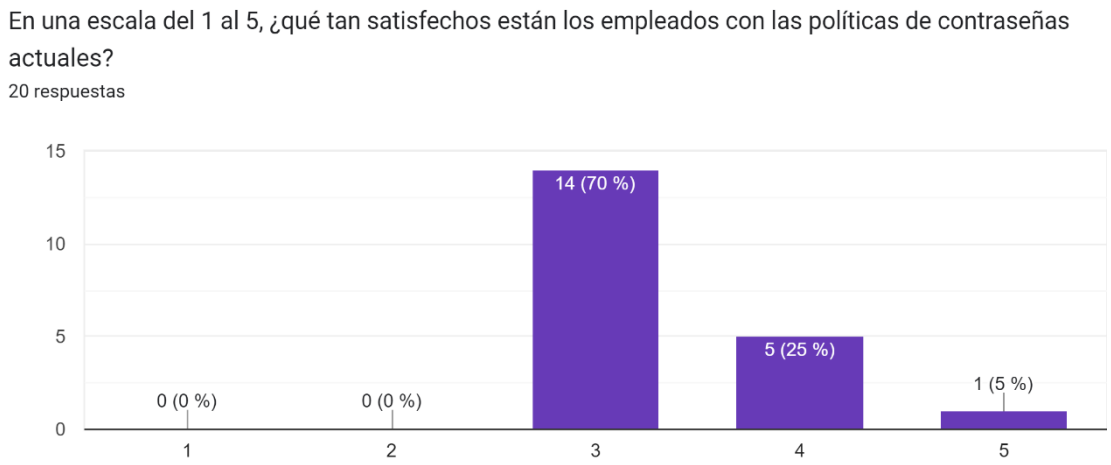


Fuente: Elaboración Propia

Se observa, según la percepción de los empleados, la mayoría no cambia sus contraseñas de acuerdo con las políticas de seguridad, pues el 95% de los votos indica no se realiza cambios. Un 5% de los encuestados menciona se realiza cambios cada seis meses, lo anterior representa una minoría que sigue las recomendaciones de cambio periódico establecidas por las políticas de seguridad.

Ilustración 15

Gráfico donde se representa las respuestas a la pregunta No. 11

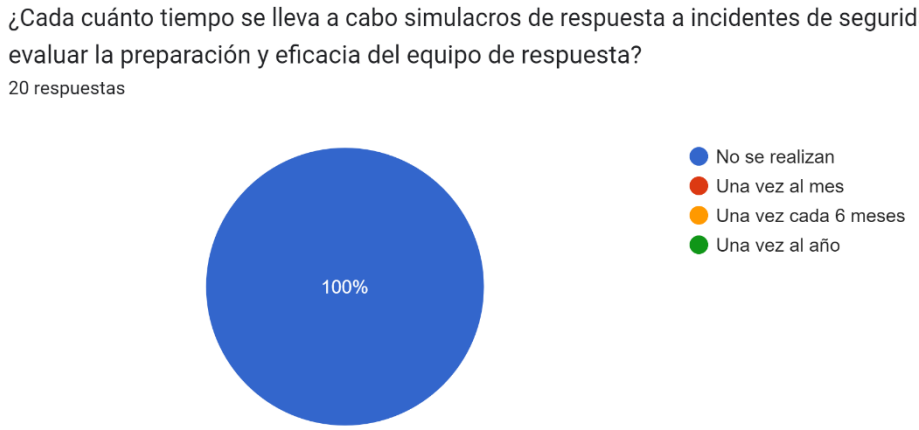


Fuente: Elaboración Propia

Se observa la evaluación de los empleados respecto de su nivel de satisfacción con las políticas de contraseñas actuales. El 70% de los encuestados indica que su nivel de satisfacción es regular, esto sugiere la existencia de un porcentaje considerable de empleados quienes podrían tener mejores expectativas en relación con estas políticas. Un 25% manifiesta estar satisfecho, indicando un grado de aceptación. Además, un 5% expresa estar muy satisfecho, lo cual sugiere hay una pequeña parte que se muestra altamente conforme con las políticas de contraseñas implementadas.

Ilustración 16

Gráfico donde se representa las respuestas a la pregunta No. 12

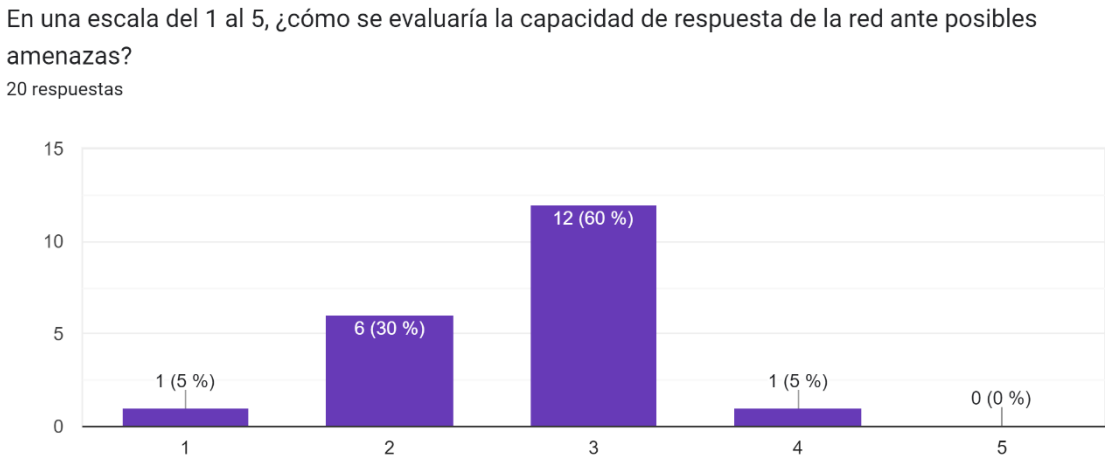


Fuente: Elaboración Propia

Se observa no se lleva a cabo simulacros de respuesta a incidentes de seguridad de red para evaluar la preparación y eficacia del equipo de respuesta, pues la totalidad, es decir, el 100% de los votos, indica no se realiza dichos simulacros. La implementación de simulacros puede ser considerada para fortalecer la preparación del equipo y mejorar la respuesta ante incidentes de seguridad.

Ilustración 17

Gráfico donde se representa las respuestas a la pregunta No. 13

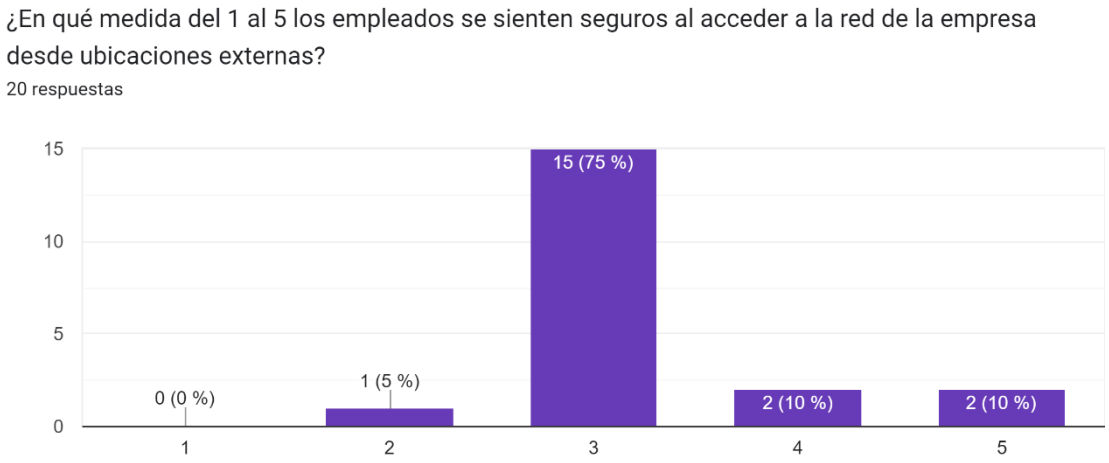


Fuente: Elaboración Propia

Se observa la percepción de los empleados en cuanto a la capacidad de respuesta de la red ante posibles amenazas. Un 5% la califica como muy mala, señala una preocupación significativa en relación con la efectividad de la red para hacer frente a amenazas. El 30% la considera mala, indica hay una proporción adicional que percibe limitaciones en la capacidad de respuesta. Un 60% la clasifica como regular, sugiere que la mayoría de los empleados tiene una capacidad media de la red para hacer frente a amenazas. Por último, un 5% la percibe como buena, lo cual indica hay una pequeña parte quien tiene una opinión positiva sobre la capacidad de respuesta de la red.

Ilustración 18

Gráfico donde se representa las respuestas a la pregunta No. 14

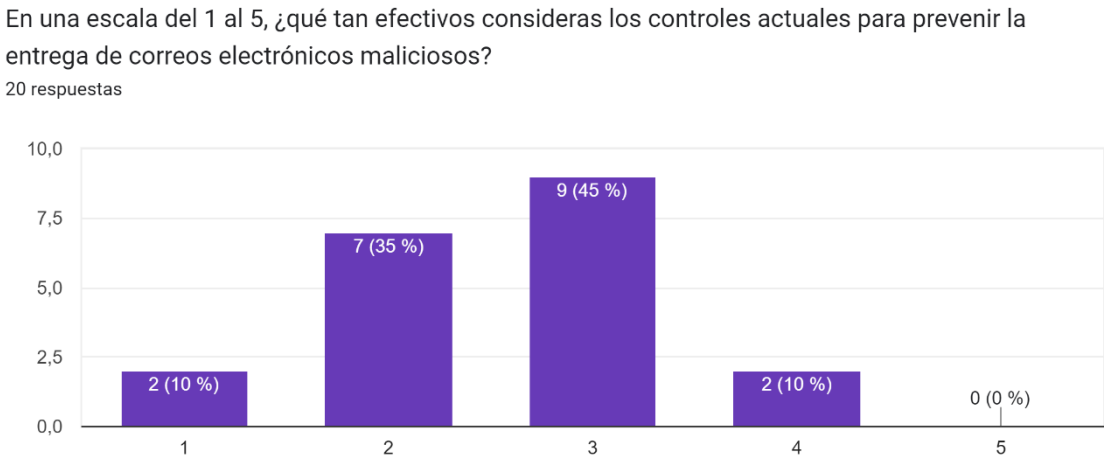


Fuente: Elaboración Propia

Se observa la percepción de los empleados acerca de su seguridad al acceder a la red de la empresa desde ubicaciones externas. Un 5% manifiesta sentirse inseguro, lo anterior indica una preocupación mínima respecto de la seguridad de dichos accesos. El 75% lo califica como regular, sugiriendo que la mayoría tiene una percepción intermedia en cuanto a su seguridad. Un 10% se siente seguro, eso indica un grado de confianza por parte de este grupo. Además, otro 10% se considera muy seguro, lo cual sugiere hay una pequeña parte que tiene una alta confianza en la seguridad de los accesos remotos.

Ilustración 19

Gráfico donde se representa las respuestas a la pregunta No. 15

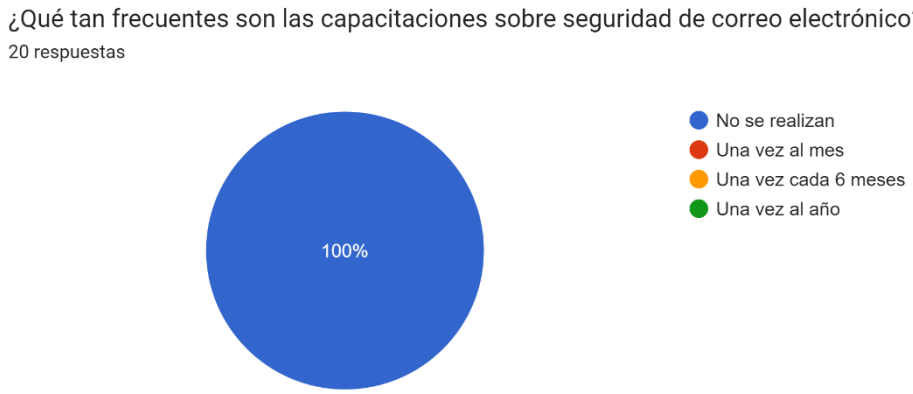


Fuente: Elaboración Propia

Se observa la percepción de los empleados respecto de la efectividad de los controles actuales para prevenir la entrega de correos electrónicos maliciosos. Un 10% de los votantes se sienten muy inseguros, indicando una preocupación significativa acerca de la eficacia de los controles. El 35% se considera inseguro, eso señala una proporción adicional con inquietudes sobre la seguridad de los correos electrónicos recibidos. Un 45% lo califica como regular, ello sugiere que la mayoría tiene una evaluación intermedia en cuanto a la eficacia de los controles. Finalmente, el 10% se siente seguro, indicando un grado de confianza por parte de este grupo.

Ilustración 20

Gráfico donde se representa las respuestas a la pregunta No. 16

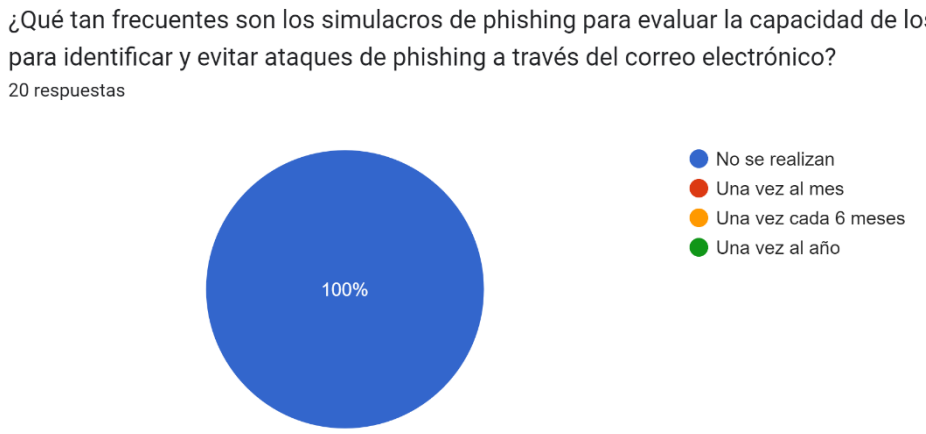


Fuente: Elaboración Propia

Se observa no se llevan a cabo capacitaciones sobre seguridad de correo electrónico, pues la totalidad, es decir, el 100% de los participantes, indica no se realiza dichas capacitaciones. La falta de capacitación puede representar un riesgo potencial, pues los empleados pueden no estar completamente informados sobre las amenazas y mejores prácticas asociadas con la seguridad de los correos electrónicos.

Ilustración 21

Gráfico donde se representa las respuestas a la pregunta No. 17



Fuente: Elaboración Propia

Se observa no se llevan a cabo simulacros de phishing con el fin de evaluar la capacidad de los empleados para identificar y evitar ataques de phishing a través del correo electrónico, por cuanto la totalidad, es decir, el 100% de las respuestas, indican no

se realiza dichos simulacros. La implementación de simulacros de phishing puede ayudar a los empleados y fortalecer sus habilidades para identificar amenazas cibernéticas.

Entrevista

En el análisis de las políticas para la restricción de navegación en internet, es fundamental destacar la ausencia de incidentes significativos hasta el momento, lo cual sugiere que las restricciones actuales brindan un nivel razonable de seguridad en el entorno digital de la organización. No obstante, durante la entrevista, el participante expresa la necesidad de considerar medidas adicionales para fortalecer aún más la seguridad y, prevenir posibles ataques o accesos no autorizados. Este planteamiento resalta la importancia de una revisión y actualización de las políticas de navegación.

En lo respectivo al control de acceso y criptografía, se observa: a pesar de la falta de sesiones informativas, los empleados desarrollan un entendimiento ético sobre las políticas de seguridad en vigor. Sin embargo, la entrevista pone de manifiesto que la ausencia de sesiones formativas puede convertirse en un obstáculo para garantizar todos los miembros del personal estén completamente informados y al tanto de las políticas de seguridad. En este sentido, se sugiere la implementación de programas de capacitación los cuales no solo refuercen el entendimiento ético existente, sino también aseguren la plena comprensión y adherencia a las políticas de seguridad de la empresa.

En el ámbito del control de credenciales y permisos, se destaca la aplicación de un proceso estructurado para desactivar las cuentas de empleados quienes abandonan la organización, esto es un paso crucial en la gestión de accesos. No obstante, surge la preocupación en torno al riesgo potencial asociado con la práctica de compartir credenciales a través de canales no seguros, como WhatsApp o correo electrónico. En respuesta, se plantea la consideración de métodos más seguros para transmitir esta información confidencial, entre ellos el empleo de plataformas cifradas. Se garantiza así un nivel elevado de seguridad en la gestión de credenciales.

En lo concerniente al control de seguridad en usuarios, el informe destaca la falta de inconvenientes con las contraseñas hasta el momento. Sin embargo, se resalta la importancia de implementar prácticas regulares de evaluación de contraseñas y la necesidad de abordar la ausencia de medidas para contrarrestar contraseñas débiles. Este

análisis resalta la relevancia de mantener un enfoque proactivo en la gestión de contraseñas, asegurando la robustez de las medidas de seguridad en este aspecto crucial.

En el ámbito de la seguridad en la red, la inexistencia de problemas se interpreta como un indicador positivo de la efectividad de las medidas de seguridad implementadas en la infraestructura de red. Sin embargo, se plantea la sugerencia de realizar evaluaciones de seguridad con mayor periodicidad. Esta recomendación se fundamenta en la premisa de que la ausencia de situaciones de amenazas no garantiza una seguridad total y la preparación ante posibles amenazas futuras se fortalece mediante evaluaciones regulares y actualizaciones en el enfoque de seguridad de red.

Finalmente, en el control y prevención de correos electrónicos, se destaca la ausencia de ataques de phishing exitosos hasta la fecha. Sin embargo, se resalta la necesidad de mejorar la educación sobre los riesgos asociados con correos electrónicos maliciosos. Este análisis sugiere la implementación de programas de capacitación que fortalezcan la conciencia de los empleados en relación con las amenazas de phishing, garantizando así una postura más robusta frente a posibles ataques.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

Conclusiones

La política de restricción para la navegación en internet establece directrices claras para garantizar un uso responsable y enfocado en los objetivos laborales de los recursos digitales de la organización. Al adherirse a los estándares de seguridad de la norma ISO/IEC 27001, se promueve la integridad de la información y se fortalece la protección contra posibles amenazas cibernéticas. Además, al implementar medidas como el acceso controlado, la restricción de contenido, el monitoreo activo y la formación continua, se crea un ambiente seguro y productivo para el personal.

El procedimiento de Control de Acceso y Criptografía establece medidas cruciales para salvaguardar la información sensible de la entidad, cumpliendo con los estándares de seguridad de la norma ISO/IEC 27001. Al enfocarse en el cifrado, el control de acceso, el registro y auditoría, así como la capacitación de los usuarios, se crea un entorno más seguro y confiable para la gestión de la información. Estas medidas no solo protegen los datos en reposo y en tránsito, sino también garantizan el acceso a la información esté restringido y controlado adecuadamente.

El procedimiento de Control de Credenciales y Permisos es fundamental para garantizar la seguridad de la información dentro de la empresa, cumpliendo con los estándares establecidos en la norma ISO/IEC 27001. A través de la implementación de este procedimiento, se establece medidas claras para la gestión de accesos de usuarios, desde la solicitud inicial hasta la retirada o reasignación de derechos de acceso. Además, se promueve la conciencia de seguridad entre los empleados mediante programas de capacitación y, se asegura la trazabilidad de las actividades a través de registros y auditorías periódicas.

El procedimiento de Control de Seguridad en Usuarios establece directrices claras y específicas para garantizar la creación, gestión y protección adecuada de contraseñas dentro de la empresa, en línea con los estándares de seguridad establecidos por la norma ISO/IEC 27001. Al implementar este procedimiento se fortalece significativamente la seguridad de los sistemas y aplicaciones, se reduce el riesgo de accesos no autorizados y protege la información confidencial de la empresa y sus clientes.

El procedimiento de Control y Prevención de Correo Electrónico es fundamental para salvaguardar la seguridad de la información y protegerse contra amenazas como el phishing. Este conjunto de medidas, abarca desde la adquisición de soluciones tecnológicas hasta la capacitación del personal, garantiza una defensa integral contra ataques cibernéticos dirigidos a través del correo electrónico. Al seguir este procedimiento, la organización puede fortalecer su postura de seguridad, cumplir con los estándares de la norma ISO/IEC 27001 y mitigar los riesgos asociados con la ingeniería social y la suplantación de identidad.

La implementación de medidas de seguridad en la red conforme con los requisitos de la norma ISO/IEC 27001, es esencial para garantizar la protección de los datos e información de una organización. Desde firewalls hasta sistemas de detección de intrusos y redes privadas virtuales, cada una de estas medidas desempeña un papel fundamental en la creación de un entorno seguro y confiable. El monitoreo continuo y el registro de eventos también son aspectos críticos para detectar y responder rápidamente a posibles incidentes de seguridad.

Recomendaciones

La responsabilidad de implementar la política de restricción de navegación a internet recae en el encargado del área de Seguridad de la Información, quien debe asegurarse de su correcta aplicación y cumplimiento. Es fundamental esta persona tenga un profundo conocimiento de los estándares de seguridad y las necesidades específicas de la organización. Se recomienda la elaboración y revisión de esta política se realice de manera meticulosa, considerando tanto los requisitos de seguridad como las necesidades operativas del negocio. Dependiendo de la complejidad de la infraestructura de la red y las políticas internas de la organización, la elaboración de esta política puede tomar entre dos semanas y un mes, incluyendo el tiempo necesario para la revisión por parte de las partes interesadas y su aprobación final. Es crucial este proceso no se apresure para garantizar que todas las consideraciones pertinentes sean tomadas en cuenta y la política resultante sea efectiva y viable en el contexto organizacional.

Es perentorio asignar un responsable de seguridad de la información, para supervisar y ejecutar el procedimiento de Control de Acceso y Criptografía de manera efectiva. Se recomienda que un equipo donde se incluya expertos en seguridad de la información, sea

designado para llevar a cabo estas tareas. Además, se sugiere establecer plazos claros para cada medida dentro del procedimiento. En particular, la revisión de privilegios de usuario debe realizarse al menos cada seis meses para garantizar su actualización y relevancia. El responsable de seguridad de la información debe dedicar tiempo suficiente para completar cada tarea de manera meticulosa, con el objetivo de mantener un nivel óptimo de seguridad en todo momento.

Es recomendable asignar la responsabilidad de la gestión del procedimiento de Control de Credenciales y Permisos a un equipo de seguridad de la información o a un administrador de sistemas, quien cuente con el conocimiento y la experiencia necesarios para llevar a cabo estas tareas de manera efectiva. Además, se sugiere establecer tiempos específicos para la realización de cada etapa del procedimiento, asegurando así, los procesos se lleven a cabo de manera oportuna y eficiente. Se estima que la implementación completa del procedimiento, desde la solicitud inicial hasta la realización de auditorías periódicas, puede tardar aproximadamente de 2 a 4 semanas.

Se recomienda el responsable de Seguridad de la Información sea el encargado de supervisar y garantizar, la implementación efectiva del procedimiento de Control de Seguridad en Usuarios. La revisión y actualización anual, así como la realización de auditorías periódicas cada seis meses, deben ser responsabilidad del responsable de Seguridad de la Información o del equipo de seguridad designado. Dada la importancia de mantener la seguridad de forma continua, se sugiere asignar recursos suficientes para realizar estas tareas de manera oportuna, garantizando así la eficacia y relevancia continua del procedimiento. Idealmente, estas revisiones y auditorías no deben tomar más de dos semanas en completarse, permitiendo una respuesta rápida a cualquier brecha de seguridad identificada.

Es esencial designar un equipo responsable de implementar y mantener este procedimiento de Control y Prevención de Correo Electrónico. Se recomienda que el equipo de seguridad de la información, en colaboración con el departamento de tecnología de la información, asuma esta responsabilidad. Este equipo debe contar con los recursos necesarios y el apoyo de la alta dirección para llevar a cabo las tareas en el procedimiento de manera efectiva. Además, se recomienda establecer un cronograma claro para la ejecución y revisión periódica de este procedimiento. Idealmente, la implementación

inicial del procedimiento debe completarse en un plazo de uno a dos meses, con revisiones regulares cada seis meses para garantizar su eficacia continua y realizar ajustes según sea necesario.

CAPÍTULO VI: PROPUESTA

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA INFORMÁTICA

Propuesta para la protección de datos, basado en las normas ISO/IEC 27001, para la empresa Landergren Consulting Group, Ubicada en Guachipelín de Escazú

MODALIDAD PROYECTO PARA OPTAR POR EL

GRADO DE BACHILLER EN INGENIERÍA EN SISTESMAS DE INFORMACIÓN

ANDREY MORA FONSECA

San José, Costa Rica

ABRIL, 2023

La empresa Landergren Consulting Group (LCG), especializada en cierres fiscales, aperturas bancarias y gestión de recursos humanos, se destaca como uno los principales despachos expertos en contabilidad, opera con una plantilla de 21 empleados comprometidos.

Surge un problema con múltiples áreas, pues no cuentan con las debidas restricciones para navegar por internet, lo cual pone a la empresa en riesgo frente a potenciales amenazas cibernéticas. Los empleados corren un mayor riesgo al acceder a sitios maliciosos, debido al uso indiscriminado que hacen de la red. Lo anterior puede generar vulnerabilidades y exponerlos a posibles ataques informáticos.

Por otra parte, la inexistencia de controles adecuados de seguridad, así como políticas y procedimientos relacionados, genera una deficiencia en la gobernabilidad, la cual propicia el robo, divulgación indebida, alteración y pérdida potencialmente dañina para información confidencial. Además, cuando se carece de políticas adecuadas para proteger las contraseñas se deja vulnerable a la empresa ante potenciales ataques cibernéticos, permitiendo un acceso sin permiso y una eventual sustracción indebida de información.

Existe una preocupación constante por la seguridad en línea, por cuanto no se ha implementado las suficientes precauciones para salvaguardar los datos y el material informativo corporativo. Por consiguiente, existe un riesgo real de sufrir ciberataques al sistema.

Ante este escenario, el objetivo general de este estudio es diseñar una propuesta de mejora basada en la norma ISO/IEC 27001, centrada en la seguridad de datos e información del sistema contable de LCG. Los objetivos específicos incluyen la creación de políticas de restricción de navegación, la construcción de procedimientos para proteger y controlar los dispositivos, la implementación de medidas de seguridad de usuarios y el análisis de la protección de datos, todos alineados con la norma ISO/IEC 27001.

Por lo tanto, la justificación de esta investigación radica en la importancia crucial de la seguridad de la información en el actual entorno empresarial. Proteger datos críticos, garantizar el cumplimiento normativo y mantener la confianza del cliente, son elementos esenciales en un mundo de amenazas cibernéticas en constante evolución. Los resultados

de esta investigación prometen beneficios que van desde mejorar la seguridad y el cumplimiento normativo, hasta fortalecer la reputación empresarial y proteger la confianza de los clientes, con impactos positivos a nivel empresarial, social y ético.

En cuanto a las proyecciones, la investigación busca mejorar la seguridad de los datos en los sistemas contables de la empresa, garantizar el cumplimiento normativo, proteger la reputación y reducir los riesgos financieros asociados con incidentes de seguridad. El alcance funcional abarca desde la evaluación de riesgos, hasta la implementación de políticas y procedimientos, mientras el alcance tecnológico se enfocará en evaluar y recomendar soluciones para fortalecer la seguridad del sistema contable.

La propuesta presente en este documento consiste en diseñar y aplicar una política de restricción para la navegación. Este enfoque no solamente protegerá la infraestructura digital, sino además asegurará un acceso exclusivo a internet con propósitos relacionados con el trabajo.

Con base en los lineamientos recomendados por la ISO/IEC 27001, esta propuesta busca asegurar un adecuado control, tanto del acceso a redes como al uso de servicios. Con este propósito, se pretende realizar una supervisión exhaustiva y tomar medidas preventivas al bloquear o limitar el acceso a sitios web relacionados con entretenimiento, que podría presentar una amenaza para la integridad y fiabilidad de la infraestructura.

El objetivo es delinear claramente los límites, más que imponer restricciones. La política de navegación no busca suprimir la libertad, sino dirigirla hacia fines laborales beneficiosos. Así cada clic realizado se convierte en una valiosa contribución para alcanzar las metas institucionales.

Política de Restricción de Navegación a Internet

Objetivo

El propósito de esta política es establecer directrices claras para restringir la navegación en la red de la organización, de conformidad con los estándares de seguridad de la norma ISO/IEC 27001. Se busca salvaguardar la integridad de la información y promover el uso responsable de los recursos digitales, enfocando el acceso a internet hacia fines laborales.

Alcance

Esta política se aplica a todos los empleados, contratistas y, cualquier otra persona que tenga acceso a la red de la organización.

Directrices de Restricción

Acceso Controlado

Se permitirá el acceso a internet exclusivamente con fines laborales.

Los empleados deberán utilizar sus credenciales individuales para acceder a la red.

Se implementará un control de acceso riguroso para asegurar la autenticación y autorización adecuadas.

Restricción de Contenido

Se bloqueará o restringirá el acceso a páginas web, las cuales no estén directamente relacionadas con las responsabilidades laborales.

El contenido de entretenimiento, juegos y redes sociales será específicamente restringido para preservar la productividad y la seguridad de la red.

Monitoreo Activo

La red será monitoreada de manera continua para identificar patrones de acceso y posibles amenazas.

Cualquier actividad sospechosa será investigada y abordada de inmediato.

Formación y Concientización

Se proporcionará formación regular a los empleados sobre las políticas de navegación y las razones detrás de estas restricciones.

La concientización sobre la seguridad informática se fomentará como parte integral de la cultura organizacional.

Responsabilidad del Usuario

Los empleados son responsables de utilizar los recursos digitales de manera ética y conforme con las políticas establecidas.

El incumplimiento de estas directrices puede resultar en acciones disciplinarias, incluyendo la suspensión del acceso a la red.

Revisión y Actualización

Esta política será revisada anualmente para asegurar su relevancia y eficacia. Cualquier cambio significativo en la infraestructura de la red será seguido por una actualización inmediata de esta política.

Esta política entra en vigor a partir de la fecha de su aprobación y será comunicada a todos los miembros de la organización.

Firma del responsable de Seguridad de la Información: _____

Fecha de aprobación: _____

Con el fin promover el uso responsable y enfocado en objetivos laborales del internet por parte del personal, se establecerá políticas restrictivas basadas en los estándares ISO/IEC 27001.

Estas medidas no solo aseguran el cumplimiento de estándares internacionales, sino también crean un ambiente digital seguro, en el cual tanto la productividad como la protección de datos sensitivos convergen sin dificultades.

Política de Control de Acceso y Criptografía

Objetivo

El propósito de esta política es establecer directrices claras para proteger y controlar los dispositivos que acceden a la información de la entidad, de conformidad con los estándares de seguridad de la norma ISO/IEC 27001. Se busca salvaguardar la integridad de la información mediante el uso de técnicas de cifrado y definir los privilegios de usuarios en relación con las aplicaciones y la información.

Alcance

Esta política se aplica a todos los dispositivos que acceden a la información de la empresa, incluyendo computadoras de escritorio, portátiles, dispositivos móviles y cualquier otro equipo que almacene, procese o transmita datos relevantes.

Directrices de Protección y Control

Cifrado

Seleccionar un algoritmo de cifrado aprobado por la organización, para proteger la información.

Implementar el cifrado en los dispositivos y sistemas de almacenamiento.

Gestionar las claves de cifrado de forma segura y restringir el acceso a estas.

Control de Acceso

Definir roles de usuario para controlar el acceso a aplicaciones e información.

Asignar privilegios a los roles de usuario según sus necesidades de acceso.

Revisar periódicamente los privilegios de usuario para garantizar su adecuación.

Registro y Auditoría

Definir eventos que se registrará relacionados con el acceso a la información.

Implementar registro de eventos en dispositivos y sistemas.

Realizar auditorías periódicas de registros para detectar actividades sospechosas.

Capacitación

Desarrollar un programa de capacitación sobre medidas de seguridad y responsabilidades.

Impartir capacitación periódica a los empleados.

Evaluar la efectividad de la capacitación mediante pruebas y evaluaciones.

Responsabilidades

El equipo de seguridad de la información será responsable de supervisar y hacer cumplir esta política.

Los gerentes de departamento serán responsables de garantizar que sus equipos cumplan con las medidas de seguridad establecidas.

Todos los empleados deben cumplir con esta política y participar en la capacitación proporcionada.

Cumplimiento

El incumplimiento de esta política puede resultar en acciones disciplinarias, incluida la suspensión del acceso a la red, además de acciones legales según corresponda.

Revisión y Actualización

Esta política se revisará anualmente para asegurar su relevancia y eficacia. Cualquier cambio significativo en la infraestructura de seguridad será seguido por una actualización inmediata de esta política.

Fecha de aprobación: _____

Firma del responsable de Seguridad de la Información: _____

Política de Control de Credenciales y Permisos

Objetivo

El propósito de esta política es garantizar la seguridad de la información al establecer directrices claras para la gestión de acceso de usuarios, de acuerdo con los estándares de seguridad de la norma ISO/IEC 27001. Se enfoca en la retirada o reasignación de derechos de acceso al personal que abandona la empresa, así como en la asignación adecuada de permisos para preservar la integridad de los datos.

Alcance

Esta política se aplica a todos los empleados, contratistas y cualquier otra persona quien requiera acceso a los sistemas y datos de la organización.

Directrices

Solicitud de Acceso

Se desarrollará un formulario de solicitud de acceso donde se recoja información detallada sobre el usuario, su función en la empresa, las necesidades de acceso y la justificación para la solicitud.

El proceso de aprobación será definido claramente, indicando quién es responsable de aprobar las solicitudes y los criterios utilizados para la aprobación.

Asignación de Permisos

Se definirá roles de usuario basados en las responsabilidades y necesidades de acceso.

Los permisos de acceso serán asignados de la manera mínima necesaria para el desempeño de las funciones del usuario.

Retirada o Reasignación de Acceso

Se establecerá condiciones para la retirada o reasignación de derechos de acceso, como el cese de la relación laboral o cambios en las responsabilidades del usuario.

Se definirá un proceso para notificar al usuario sobre la retirada o reasignación de sus derechos de acceso y cómo se eliminará o modificará sus permisos.

Capacitación

Se desarrollará un programa de capacitación el cual abarque las políticas de seguridad, las responsabilidades de los usuarios y las mejores prácticas para proteger la información.

La capacitación será impartida a todos los usuarios quienes requieran acceso a los sistemas y datos de la organización.

Registro y Auditoría

Se definirá los eventos por registrar, incluyendo inicios de sesión, accesos a datos sensibles y cambios en la configuración de cuentas.

Se implementará un sistema de registro de eventos y se realizará auditorías periódicas para detectar actividades sospechosas y garantizar el cumplimiento de las políticas establecidas.

Responsabilidades

El equipo de seguridad de la información será responsable de supervisar y hacer cumplir esta política.

Los gerentes de departamento serán responsables de garantizar sus equipos cumplan con las medidas de seguridad establecidas.

Todos los empleados deben cumplir con esta política y participar en la capacitación proporcionada.

Cumplimiento

El incumplimiento de esta política puede resultar en acciones disciplinarias, incluida la suspensión o revocación del acceso a los sistemas y datos de la organización.

Revisión y Actualización

Esta política se revisará anualmente para asegurar su relevancia y eficacia en la protección de la información. Cualquier cambio significativo en los procesos de gestión de acceso será seguido por una actualización inmediata de esta política.

Fecha de Aprobación: _____

Firma del responsable de Seguridad de la Información: _____

Política de Control de Seguridad en Usuarios

Objetivo

El propósito de esta política es establecer pautas claras para la creación y gestión de contraseñas seguras, garantizando un control de acceso efectivo a los sistemas y aplicaciones de la empresa de contabilidad, conforme con la norma ISO/IEC 27001.

Alcance

Esta política se aplica a todos los empleados, contratistas y cualquier otra persona quien requiera acceso a los sistemas y aplicaciones de la empresa de contabilidad.

Directrices

Definición de Políticas de Contraseñas

Todas las contraseñas deben cumplir con los siguientes requisitos mínimos:

- Longitud mínima de ocho caracteres.
- Inclusión de al menos una letra mayúscula.
- Inclusión de al menos una letra minúscula.
- Inclusión de al menos un número.
- Inclusión de al menos un carácter especial (por ejemplo: !, @, #, $, %, etc.).

Se prohíbe el uso de información personal (nombres, fechas de nacimiento y otros.) como parte de las contraseñas.

Creación de Contraseñas

Al crear una nueva contraseña, el usuario debe seguir las políticas definidas.

Se recomienda el uso de frases o combinaciones de palabras para aumentar la complejidad.

Cambio Regular de Contraseñas

Todos los usuarios deben cambiar sus contraseñas cada 90 días.

Las contraseñas no pueden repetirse con las utilizadas anteriormente.

Almacenamiento Seguro de Contraseñas

Prohibido almacenar contraseñas en documentos no seguros, por medios no cifrados.

Se debe utilizar soluciones de gestión de contraseñas seguras y aprobadas por la empresa.

Bloqueo de Cuenta por Intentos Fallidos

Después de tres intentos fallidos de inicio de sesión, la cuenta del usuario debe bloquearse temporalmente.

La duración del bloqueo debe ser de al menos diez minutos.

Auditoría Regular

Realizar auditorías periódicas cada seis meses para evaluar el cumplimiento de las políticas de contraseñas.

Registrar y analizar los intentos de inicio de sesión, bloqueos de cuenta y cambios de contraseñas.

Capacitación de Usuarios

Proporcionar capacitación regular cada seis meses sobre la importancia de contraseñas seguras y las políticas establecidas.

Informar sobre las consecuencias de compartir contraseñas y la responsabilidad individual en la seguridad de la información.

Revisión Continua

Este procedimiento será revisado y actualizado anualmente o según sea necesario para reflejar los cambios en las amenazas de seguridad y las mejores prácticas.

Documentación y Registro

Mantener registros detallados de cambios de contraseñas, bloqueos de cuentas y auditorías de seguridad.

Responsabilidades

El equipo de seguridad de la información será responsable de supervisar y hacer cumplir esta política.

Los gerentes de departamento serán responsables de garantizar que sus equipos cumplan con las medidas de seguridad establecidas.

Todos los empleados deben cumplir con esta política y participar en la capacitación proporcionada.

Cumplimiento

El incumplimiento de esta política puede resultar en acciones disciplinarias, incluida la suspensión o revocación del acceso a los sistemas y datos de la organización.

Revisión y Actualización:

Esta política será revisada anualmente para asegurar su relevancia y eficacia en la protección de la información. Cualquier cambio significativo en los procesos de gestión de acceso será seguido por una actualización inmediata de esta política.

Fecha de Aprobación: _____

Firma del responsable de Seguridad de la Información: _____

Política de Control y Prevención de Correo Electrónico

Objetivo

El propósito de esta política es establecer directrices claras para el control de correo electrónico y la prevención de ataques de phishing, en línea con los estándares de seguridad de la norma ISO/IEC 27001. Esta política tiene como objetivo salvaguardar la integridad de los sistemas de correo electrónico y proteger la información confidencial de la empresa.

Alcance

Esta política se aplica a todos los empleados, contratistas y cualquier otro individuo quien utilice el correo electrónico dentro de la empresa.

Directrices

Implementación de Filtrado de Correo Electrónico

Se adquirirá e implementará una solución de filtrado de correo electrónico, la cual detecte y bloquee correos no deseados, sospechosos o maliciosos.

Se configurará reglas de filtrado personalizadas para identificar y bloquear posibles intentos de phishing.

Uso de Antivirus y Antimalware

Se instalará y mantendrá actualizado un software antivirus y antimalware en todos los dispositivos utilizados para el correo electrónico.

Se programará análisis regulares de correo electrónico y archivos adjuntos para detectar y eliminar posibles amenazas.

Autenticación de Correo Electrónico (SPF, DKIM, DMARC)

Se configurará registros SPF (Sender Policy Framework) para verificar la autenticidad del remitente y prevenir la suplantación de identidad.

Se implementará DKIM (DomainKeys Identified Mail) para firmar digitalmente los correos electrónicos salientes y garantizar su integridad.

Se configurará DMARC (Domain-based Message Authentication, Reporting, and Conformance) para establecer políticas de autenticación y recibir informes sobre intentos de phishing.

Respuesta a Incidentes de Phishing

Se establecerá un protocolo de respuesta a incidentes de phishing que incluya la notificación inmediata a los equipos de seguridad y TI.

Se realizará investigaciones internas para determinar el alcance del ataque de phishing y tomar medidas correctivas para mitigar el impacto.

Monitoreo y Evaluación Continua

Se implementará sistemas de monitoreo continuo para supervisar el tráfico de correo electrónico en busca de actividades sospechosas o intentos de phishing.

Se llevará a cabo evaluaciones periódicas de la efectividad de las medidas de control de correo electrónico y se ajustará los procedimientos según sea necesario.

Capacitación y Concientización del Personal

Se impartirá sesiones de capacitación regulares sobre la identificación de correos electrónicos fraudulentos y técnicas de ingeniería social utilizadas en ataques de phishing.

Se fomentará una cultura de seguridad cibernética entre los empleados, alentándolos a reportar cualquier correo electrónico sospechoso o actividad inusual.

Documentación y Mejora Continua

Se documentará todos los procedimientos relacionados con el control de correo electrónico y la prevención de phishing, incluyendo políticas, registros de incidentes y acciones tomadas.

Se llevará a cabo revisiones periódicas de la política y se actualizará conforme con cambios en las amenazas de seguridad y las mejores prácticas.

Responsabilidades

El equipo de seguridad de la información será responsable de supervisar y hacer cumplir esta política.

Todos los usuarios deben cumplir con esta política y participar en la capacitación proporcionada.

Cumplimiento

El incumplimiento de esta política puede resultar en acciones disciplinarias, incluida la suspensión o revocación del acceso a los sistemas y datos de la organización.

Revisión y Actualización

Esta política será revisada anualmente para asegurar su relevancia y eficacia en la protección de la información. Cualquier cambio significativo en las medidas de seguridad será seguido por una actualización inmediata de esta política.

Fecha de Aprobación: _____

Firma del responsable de Seguridad de la Información: _____

El objetivo central radica en crear un procedimiento donde se garantice y supervise los dispositivos de información, siguiendo las indicaciones señaladas por la norma ISO/IEC 27001.

La propuesta presente en este documento contempla el diseño e implementación de medidas prácticas que se adhieran a los principios establecidos en la norma ISO/IEC 27001, garantizando así una adecuada protección de datos tanto mientras están estáticos, como mientras circulan por redes.

La clave de este resguardo reside en el arte del cifrado, una técnica potente que transforma nuestra información en un código incomprensible para aquellos quienes intentan espiar o robar la información.

Procedimiento de Control de Acceso y Criptografía

Objetivo

Este procedimiento tiene como objetivo establecer medidas efectivas para proteger y controlar los dispositivos que acceden a la información de la entidad, de acuerdo con los estándares de seguridad de la norma ISO/IEC 27001. Se enfoca en el uso de técnicas de cifrado para resguardar la información en reposo y en tránsito, así como en definir los privilegios de usuarios en relación con las aplicaciones y la información.

Alcance

Este procedimiento aplica a todos los dispositivos que acceden a la información de la organización, incluyendo computadoras de escritorio, portátiles, dispositivos móviles y cualquier otro equipo que almacene, procese o transmita datos relevantes.

Medidas de Protección y Control

1.Cifrado

Seleccionar un algoritmo de cifrado: Seleccionar un algoritmo de cifrado aprobado por la organización y adecuado para el tipo de información que se va a proteger.

Implementar el cifrado: Implementar el cifrado en los dispositivos y sistemas de almacenamiento.

Gestionar las claves de cifrado: Almacenar las claves de cifrado de forma segura y restringir el acceso a estas.

2.Control de acceso

Definir los roles de usuario: Definir los roles de usuario por utilizar para controlar el acceso a las aplicaciones e información.

Asignar privilegios a los roles: Asignar privilegios a los roles de usuario en función de sus necesidades de acceso.

Revisar los privilegios de usuario: Revisar los privilegios de usuario periódicamente para asegurarse de que siguen siendo adecuados.

3.Registro y auditoría

Definir los eventos que se registrará: Definir los eventos que se registrará relacionados con el acceso a la información.

Implementar el registro de eventos: Implementar el registro de eventos en los dispositivos y sistemas.

Realizar auditorías: Realizar auditorías periódicas cada seis meses de los registros, para detectar actividades sospechosas.

4.Capacitación

Desarrollar un programa de capacitación: Desarrollar un programa de capacitación para los usuarios sobre las medidas de seguridad y sus responsabilidades.

Impartir la capacitación: Impartir la capacitación periódica cada seis meses a los empleados.

Evaluar la eficacia de la capacitación: Evaluar la eficacia de la capacitación mediante la realización de pruebas y evaluaciones para confirmar si se está adhiriendo la información a los miembros de la organización.

Al acatar las regulaciones impuestas por el estándar ISO/IEC 27001, se diseña un proceso que resguarda eficientemente toda información mediante prácticas criptográficas avanzadas. Esto abarca tanto su almacenamiento seguro, como su transmisión segura. Se debe tener en cuenta lo siguiente: no solo la encriptación juega un papel crucial, sino también regular los privilegios de usuarios para garantizar el acceso autorizado.

El objetivo primordial es establecer una estrategia efectiva, que asegure la cancelación inmediata o reasignación adecuada de los permisos para acceder a través del sistema en el momento en el cual un empleado finaliza su vínculo con la organización.

Cuando un empleado se va de una empresa, es sumamente importante retirar o reasignar sus derechos de acceso a la plataforma. No se debe permitir que la información de valor y confidencial acabe en las manos incorrectas.

Procedimiento de Control de Credenciales y Permisos

Objetivo

Garantizar la seguridad de la información al elaborar un procedimiento que regule la gestión de acceso de usuarios, de acuerdo con los estándares establecidos en la norma

ISO/IEC 27001, con énfasis en la retirada o reasignación de derechos de acceso al personal que abandona la empresa.

1.Solicitud de acceso

Desarrollar un formulario de solicitud de acceso: El formulario debe incluir información sobre el usuario, su rol en la empresa, las necesidades de acceso a la información y la justificación para la solicitud.

Definir el proceso de aprobación: El proceso de aprobación debe definir quién es responsable de aprobar las solicitudes de acceso y qué criterios se utiliza para la aprobación.

2.Asignación de permisos

Definir los roles de usuario: Los roles de usuario deben basarse en las responsabilidades y necesidades de acceso a la información de los usuarios.

Definir los permisos de acceso: Los permisos de acceso deben ser los mínimos necesarios para que el usuario pueda realizar su trabajo.

3.Retirada o reasignación de acceso

Definir las condiciones bajo las cuales se retirará o reasignará los derechos de acceso: Las condiciones pueden incluir el cese de la relación laboral, el cambio de rol dentro de la empresa, el incumplimiento de las medidas de seguridad o la sospecha de actividad maliciosa.

Definir el proceso de retirada o reasignación de acceso: El proceso debe definir cómo se notificará al usuario sobre la retirada o reasignación de sus derechos de acceso y cómo se eliminará o modificará sus permisos.

4.Capacitación

Desarrollar un programa de capacitación: El programa de capacitación debe cubrir las medidas de seguridad del procedimiento, las responsabilidades de los usuarios y las mejores prácticas para proteger la información.

Impartir la capacitación: La capacitación debe impartirse a todos los usuarios que acceden a la plataforma.

5.Registro y auditoría

Definir los eventos que se registrará: Los eventos pueden incluir inicios de sesión, accesos a archivos sensibles, cambios en la configuración de la cuenta y actividades sospechosas.

Implementar el registro de eventos: Implementar un sistema para registrar los eventos definidos.

Realizar auditorías: Realizar auditorías periódicas de los registros para detectar actividades sospechosas.

Al seguir estos pasos, la organización estará mejor preparada para proteger su información confidencial y minimizar los riesgos asociados con la salida de empleados. La implementación exitosa de este procedimiento contribuirá significativamente a fortalecer la postura de seguridad de la empresa, en un entorno empresarial cada vez más competitivo.

Se plantea como objetivo primordial la creación de contraseñas y su gestión, se propone un marco de seguridad del usuario el cual garantice el poder y la confidencialidad. Esto significa que se construye para generar contraseñas complejas basadas en caracteres especiales, letras mayúsculas y minúsculas y números. Con un mínimo de ocho dígitos, se hace hincapié en mantener la seguridad y evitar riesgos potenciales de piratería.

Procedimiento de Control de Seguridad en Usuarios

Objetivo

Este procedimiento tiene como objetivo establecer pautas claras para la creación y gestión de contraseñas seguras, garantizando un control de acceso efectivo a los sistemas y aplicaciones de la empresa de contabilidad, conforme con la norma ISO/IEC 27001.

1. Definición de Políticas de Contraseñas

Todas las contraseñas deben cumplir con los siguientes requisitos mínimos:

- Longitud mínima de ocho caracteres.
- Inclusión de al menos una letra mayúscula.
- Inclusión de al menos una letra minúscula.

- Inclusión de al menos un número.
- Inclusión de al menos un carácter especial (por ejemplo: !, @, #, $, %, etc.).

Se prohíbe el uso de información personal (nombres, fechas de nacimiento, etc.) como parte de las contraseñas.

2. Creación de Contraseñas

Al crear una nueva contraseña, el usuario debe seguir las políticas definidas.

Se recomienda el uso de frases o combinaciones de palabras para aumentar la complejidad.

3. Cambio Regular de Contraseñas

Todos los usuarios deben cambiar sus contraseñas cada 90 días.

Las contraseñas no pueden repetirse con las utilizadas anteriormente.

4. Almacenamiento Seguro de Contraseñas

Prohibido almacenar contraseñas en documentos no seguros por medios no cifrados.

Se debe utilizar soluciones de gestión de contraseñas seguras y aprobadas por la empresa.

5. Bloqueo de Cuenta por Intentos Fallidos

Después de tres intentos fallidos de inicio de sesión, la cuenta del usuario debe bloquearse temporalmente.

La duración del bloqueo debe ser de al menos diez minutos.

6. Auditoría Regular

Realizar auditorías periódicas cada seis meses para evaluar el cumplimiento de las políticas de contraseñas.

Registrar y analizar los intentos de inicio de sesión, bloqueos de cuenta y cambios de contraseñas.

7. Capacitación de Usuarios

Proporcionar capacitación regular cada seis meses sobre la importancia de contraseñas seguras y políticas establecidas.

Informar sobre las consecuencias de compartir contraseñas y la responsabilidad individual en la seguridad de la información.

8. Revisión Continua

Este procedimiento será revisado y actualizado anualmente o según sea necesario para reflejar los cambios en las amenazas de seguridad y las mejores prácticas.

9. Documentación y Registro

Mantener registros detallados de cambios de contraseñas, bloqueos de cuentas y auditorías de seguridad.

Este procedimiento debe ser comunicado de manera clara a todos los usuarios y, la dirección de la empresa debe respaldar su implementación. La seguridad de la información es un esfuerzo conjunto, requiere la participación activa de todos los miembros de la organización.

Este procedimiento abordará aspectos clave como el filtrado de correo electrónico, el uso de herramientas antivirus y antimalware, la autenticación de correo electrónico mediante SPF, DKIM y DMARC, el establecimiento de políticas de uso de correo electrónico, la respuesta a incidentes de phishing, entre otros. Estas medidas no solo ayudarán a proteger la confidencialidad, integridad y disponibilidad de la información, sino también fortalecerán la postura de seguridad cibernética de la organización en su conjunto.

Procedimiento de Control y Prevención de Correo Electrónicos

Objetivo

Implementar medidas efectivas para el control de correo electrónico y la prevención de ataques de phishing, cumpliendo con los estándares de seguridad establecidos por la norma ISO/IEC 27001.

1. Implementación de Filtrado de Correo Electrónico

Adquirir e implementar una solución de filtrado de correo electrónico que detecte y bloquee correos no deseados, sospechosos o maliciosos.

Configurar reglas de filtrado personalizadas para identificar y bloquear posibles intentos de phishing.

2. Uso de Antivirus y Antimalware

Instalar y mantener actualizado un software antivirus y antimalware en todos los dispositivos utilizados para el correo electrónico.

Programar análisis regulares de correo electrónico y archivos adjuntos para detectar y eliminar posibles amenazas.

3. Autenticación de Correo Electrónico (SPF, DKIM, DMARC)

Configurar registros SPF (Sender Policy Framework) para verificar la autenticidad del remitente y prevenir la suplantación de identidad.

Implementar DKIM (DomainKeys Identified Mail) para firmar digitalmente los correos electrónicos salientes y garantizar su integridad.

Configurar DMARC (Domain-based Message Authentication, Reporting, and Conformance) para establecer políticas de autenticación y recibir informes sobre intentos de phishing.

4. Respuesta a Incidentes de Phishing

Establecer un protocolo de respuesta a incidentes de phishing, que incluya la notificación inmediata a los equipos de seguridad y TI.

Realizar investigaciones internas para determinar el alcance del ataque de phishing y tomar medidas correctivas para mitigar el impacto.

5. Monitoreo y Evaluación Continua

Implementar sistemas de monitoreo continuo para supervisar el tráfico de correo electrónico en busca de actividades sospechosas o intentos de phishing.

Realizar evaluaciones periódicas de la efectividad de las medidas de control de correo electrónico y ajustar los procedimientos según sea necesario.

6. Capacitación y Concientización del Personal

Impartir sesiones de capacitación regulares sobre la identificación de correos electrónicos fraudulentos y técnicas de ingeniería social utilizadas en ataques de phishing.

Fomentar una cultura de seguridad cibernética entre los empleados, alentándolos a reportar cualquier correo electrónico sospechoso o actividad inusual.

7. Documentación y Mejora Continua

Documentar todos los procedimientos relacionados con el control de correo electrónico y la prevención de phishing, incluyendo políticas, registros de incidentes y acciones tomadas.

Realizar revisiones periódicas del procedimiento y actualizarlo conforme con cambios en las amenazas de seguridad y las mejores prácticas.

Este procedimiento garantizará un nivel adecuado de seguridad en el manejo del correo electrónico, protegiendo a la organización contra amenazas como el phishing y cumpliendo con los estándares de seguridad establecidos por la norma ISO/IEC 27001. La colaboración entre los equipos de seguridad, TI y el personal será fundamental para la implementación efectiva de estas medidas.

Procedimiento de Destrucción de Medios Seguros

Objetivo

Asegurar la destrucción segura de medios que contienen información confidencial una vez que esta información ya no es necesaria, cumpliendo con los estándares de seguridad de la información y protegiendo la confidencialidad de los datos de la organización.

1. Identificación de Medios a Destruir

Todos los departamentos y empleados identificarán los medios que contienen información confidencial y ya no son necesarios para su uso.

Se registrarán estos medios en un formulario de solicitud de destrucción de medios, indicando la fecha de identificación y el motivo de la destrucción.

2. Clasificación de la Información

Antes de la destrucción, el Departamento de TI clasificará la información contenida en los medios identificados según su nivel de confidencialidad (confidencial, interna o pública).

3. Selección del Método de Destrucción

El Departamento de TI seleccionará el método de destrucción adecuado según el tipo de medio y la sensibilidad de la información contenida en el mismo.

Los métodos de destrucción pueden incluir trituración, desmagnetización, borrado seguro o incineración.

4. Ejecución de la Destrucción

Se designará un responsable del Departamento de TI para llevar a cabo la destrucción de los medios.

La destrucción se realizará en un área designada y segura, cumpliendo con los estándares de seguridad de la empresa.

5. Verificación de la Destrucción

Después de la destrucción, el responsable verificará que los medios hayan sido destruidos de manera efectiva y permanente.

Se documentará la verificación de la destrucción, incluyendo la fecha, el método utilizado y el nombre del responsable.

6. Registro y Documentación

El Departamento de TI mantendrá un registro detallado de todas las actividades relacionadas con la destrucción de medios.

La documentación se almacenará de manera segura y estará disponible para auditorías internas o externas.

7. Disposición Adecuada de los Residuos

Los residuos generados durante la destrucción se dispondrán de manera adecuada, siguiendo las regulaciones ambientales y de seguridad.

8. Auditoría y Revisión

Se realizarán auditorías periódicas para evaluar el cumplimiento de este procedimiento y su efectividad en la protección de la información confidencial.

Este procedimiento se revisará y actualizará según sea necesario para mantenerse alineado con las mejores prácticas y los cambios normativos y tecnológicos.

Este procedimiento asegurará que la información confidencial sea destruida de manera segura y efectiva, protegiendo así los intereses y la reputación de la organización.

Control de Seguridad en la Red

La protección de datos e información es fundamental para garantizar la seguridad de la información en una entidad. La norma ISO/IEC 27001 proporciona un marco de referencia para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI). De inmediato se analiza cómo se puede utilizar diferentes medidas de seguridad para cumplir con los requisitos de la norma:

Los firewalls son dispositivos de seguridad. controlan y monitorean el tráfico de red, permiten o bloquean el acceso en función de reglas predefinidas. Son esenciales para proteger la red de amenazas externas. Para cumplir con ISO/IEC 27001, se debe implementar firewalls tanto en el perímetro de la red como en segmentos internos, configurándolos adecuadamente para filtrar el tráfico no autorizado y prevenir intrusiones.

El Control de Acceso a la Red (NAC) es una solución, pues garantiza que solo los dispositivos autorizados puedan conectarse y acceder a la red. Para cumplir con ISO/IEC 27001, se debe establecer políticas de acceso donde se defina quién puede conectarse a la red y qué recursos pueden acceder. Además, se debe implementar soluciones de NAC que verifiquen la conformidad de los dispositivos antes de permitirles el acceso.

Los Sistemas de Detección de Intrusos (IDS) y los Sistemas de Prevención de Intrusos (IPS) son herramientas, las cuales monitorean la red en busca de actividades sospechosas y pueden tomar medidas para bloquear o prevenir intrusiones. Para cumplir con ISO/IEC 27001, se debe implementar IDS/IPS en puntos estratégicos de la red y configurarlos para detectar y bloquear intrusiones de acuerdo con las políticas de seguridad establecidas.

Las Redes Privadas Virtuales (VPN) proporcionan un medio seguro para que los usuarios remotos accedan a la red corporativa a través de Internet. Para cumplir con ISO/IEC 27001, se debe implementar VPN con autenticación fuerte y cifrado robusto, para proteger la confidencialidad e integridad de los datos durante la transmisión.

El monitoreo continuo de la red y el registro de eventos son aspectos críticos para detectar y responder a incidentes de seguridad de manera oportuna. Para cumplir con ISO/IEC 27001, se debe implementar herramientas de monitoreo de red que registren eventos relevantes y generen alertas ante actividades sospechosas o potencialmente maliciosas. Además, se debe mantener registros detallados de eventos de seguridad para su posterior análisis y auditoría.

REFERENCIAS

Akamai. (2023). ¿Qué es la ISO 27001? Recuperado el 27 de septiembre del 2023 del sitio web: https://www.akamai.com/es/glossary/what-is-iso-27001

Alonso, C. (2023). 10 consejos para establecer políticas para el uso de internet. Recuperado el 17 de octubre del 2023 del sitio web GlobalSuite Solutions https://www.globalsuitesolutions.com/es/10-consejos-politicas-uso-internet/#:~:text=El%20prop%C3%B3sito%20de%20una%20pol%C3%ADtica,entorno%20seguro%20y%20de%20calidad.

Araya, S. (2020). Prácticas de seguridad de la información contable. Recuperado el 27 de septiembre del 2023 del sitio web Nubox. https://blog.nubox.com/empresas/practicas-de-seguridad-de-la-informacion-contable#:~:text=malware%2C%20entre%20otros.-,%C2%BFQu%C3%A9%20es%20la%20seguridad%20en%20contabilidad%3F,trav%C3%A9s%20de%20software%20de%20seguridad.

Cloudflare. (2023). ¿Qué es la encriptación? Recuperado el 04 de octubre del 2023 del sitio web: https://www.cloudflare.com/es-es/learning/ssl/what-is-encryption/#:~:text=La%20encriptaci%C3%B3n%20es%20una%20forma%20de%20codificar%20los%20datos%20para,tambi%C3%A9n%20conocido%20como%20texto%20encriptado.

Derek DeWitt. (2022). Cifrado de datos: ¿en qué consiste? Recuperado el 04 de octubre del 2023 del sitio web Avast. https://www.avast.com/es-es/c-encryption

DocuSign. (22 abril, 2021). Auditoría de seguridad: ¿En qué consiste y cuáles son las técnicas más populares? Recuperado el 04 de octubre del 2023 del sitio web DocuSign. https://www.docusign.mx/blog/auditoria-de-seguridad

Entrust. (2023). ¿Qué es el Control de Acceso basado en Roles (RBAC)? Recuperado el 04 de octubre del 2023 del sitio web: https://www.entrust.com/es/resources/faq/what-is-role-based-access-control#:~:text=El%20control%20de%20acceso%20basado%20en%20roles%20(RBAC)%20es%20un,las%20funciones%20de%20un%20usuario.

Fernández, Y. (5 junio, 2020). RAID de discos duros: qué son y sus principales tipos. Xataka. Recuperado el 5 de diciembre del 2023 del sitio web: https://www.xataka.com/basics/raid-discos-duros-que-sus-principales-tipos

Gómez, J. A. (2023). Firewall: qué es, cómo funciona y para qué sirve.? Recuperado el 04 de octubre del 2023 del sitio web deltaprotect.

https://www.deltaprotect.com/blog/que-es-un-firewall#:~:text=La%20funci%C3%B3n%20principal%20de%20un,o%20solicitudes%20de%20entrada%20maliciosas.

Herrero, E. G. (2022). ¿Qué es una copia de seguridad y por qué debe realizarse? Recuperado el 04 de octubre del 2023 del sitio web Red Seguridad. https://www.redseguridad.com/actualidad/proteccion-de-datos-actualidad/que-es-una-copia-de-seguridad-y-por-que-debe-realizarse_20220331.html

IBM (2023). Tape Library. Recuperado el 5 de diciembre del 2023 del sitio web: https://www.ibm.com/mx-es/products/ts4300

IBM. (2023). ¿Qué es un sistema de detección de intrusiones (IDS)? Recuperado el 04 de octubre del 2023 del sitio web: https://www.ibm.com/es-es/topics/intrusion-detection-system#:~:text=Un%20sistema%20de%20detecci%C3%B3n%20de%20intrusiones%20(IDS%2C%20por%20sus%20siglas,de%20las%20pol%C3%ADticas%20de%20seguridad.

Informaticos.co. (11 noviembre, 2023). Tipos de copias de seguridad. Recuperado el 04 de octubre del 2023 del sitio web: https://informaticos.co/mantenimiento_informatico/4-tipos-de-copias-de-seguridad/

Kim Hefner. (2021). Protección de datos. Recuperado el 17 de octubre del 2023 del sitio web ComputerWeekly.es. https://www.computerweekly.com/es/definicion/Proteccion-de-datos#:~:text=La%20protecci%C3%B3n%20de%20datos%20es,a%20un%20ritmo%20sin%20precedentes.

Las fuentes de información. (s. f.). Fuentes de información. Recuperado el 17 de octubre del 2023 del sitio web: https://www.uv.es/cibisoc/tutoriales/trabajo_social/22_las_fuentes_de_informacin.html

Lorenzo, J. A. (13 mayo, 2022). Qué es la autenticación de usuario y cómo mejorar su seguridad. Recuperado el 04 de octubre del 2023 del sitio web RedesZone. https://www.redeszone.net/noticias/seguridad/que-es-autenticacion-usuario-mejorar-seguridad/

Microsoft. (2023). ¿Qué es el control de acceso? Recuperado el 17 de octubre del 2023 del sitio web https://www.microsoft.com/es-ww/security/business/security-101/what-is-access-control

Panda Security. (s. f.). Phishing: ¿qué es y cómo evitarlo? Recuperado el 04 de octubre del 2023 del sitio web: https://www.pandasecurity.com/es/security-info/phishing/#:~:text=El%20phishing%20es%20un%20m%C3%A9todo,electr%C3%B3nicos%20y%20sitios%20web%20enga%C3%B1osos.

PowerData. (2023). Seguridad de datos: en qué consiste y qué es importante en tu empresa. Recuperado el 17 de octubre del 2023 del sitio web https://www.powerdata.es/seguridad-de-datos

Sánchez, J. R. G. (s. f.). Estadística. José R. Galo Sánchez. Recuperado el 3 de noviembre del 2023 del sitio web https://proyectodescartes.org/iCartesiLibri/materiales_didacticos/IntroduccionEstadisticaProbabilidad/3ESO/2_1PoblacionMuestraRepresentativaIndividuo.html

TechTarget, (2021). Autenticación multifactor o MFA. Recuperado el 04 de octubre del 2023 del sitio web: https://www.computerweekly.com/es/definicion/Autenticacion-multifactor-o-MFA

Villanueva, A. (2021). Políticas y procedimientos de seguridad de la información. OSTEC | Segurança digital de resultados. Recuperado el 06 de octubre del 2023 del sitio web: https://ostec.blog/es/seguridad-informacion/politicas-y-procedimientos-de-seguridad-de-la-informacion/

Welink Accountants (2023). Sistema contable de una empresa: definición, características y ventajas. Recuperado el 27 de septiembre del 2023 del sitio web: https://www.welinkaccountants.es/blog/copy-sistema-contabilidad