UNIVERSIDAD INTERNACIONAL DE LAS AMERICAS
ESCUELA DE INGENIERÍA INFORMÁTICA

TRABAJO FINAL DE GRADUACIÓN PARA OPTAR POR EL GRADO DE BACHILLERATO EN INGENIERÍA DE SOFTWARE

PROPUESTA INTEGRAL DE OPTIMIZACIÓN Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA: UN ENFOQUE BASADO EN ISO/IEC 27001, ISO/IEC 27002, COBIT, NIST SP 800-46, Y MEJORES PRÁCTICAS DE ITIL

MELANNIE ANGÉLICA MORA CORRALES

CARLOS HUMBERTO AGUILAR MORA

TUTOR

Sede Central

JULIO, 2024

CONTENIDO

Tablas

Figuras

Resumen ejecutivo

El presente trabajo de graduación aborda la optimización y seguridad de la infraestructura tecnológica en la empresa CORGIA Gestión e Ingeniería Alternativa. El objetivo general consiste en diseñar una Propuesta Integral de Optimización y Seguridad de la Infraestructura Tecnológica basada en normativas internacionales y mejores prácticas. La línea teórica se fundamenta en normas como ISO/IEC 27001, ISO/IEC 27002, COBIT, NIST SP 800-46 y las Mejores Prácticas de ITIL. El enfoque metodológico incluye un análisis de la infraestructura tecnológica actual, evaluando limitaciones y riesgos asociados, así como la propuesta de soluciones específicas para mejorar la gestión de seguridad de la información y optimizar procesos operativos.

Los participantes involucrados son el equipo directivo de CORGIA, clave en la implementación y ejecución de las recomendaciones propuestas. La principal conclusión destaca la urgente necesidad de modernizar la infraestructura tecnológica y fortalecer la seguridad de la información para garantizar la continuidad del negocio y mitigar riesgos potenciales. Como recomendación principal, se sugiere la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) robusto y eficiente, alineado con las normativas internacionales mencionadas, como estrategia clave para asegurar la protección de activos de información y mejorar la eficiencia operativa de CORGIA.

CAPÍTULO I: INTRODUCCIÓN

Planteamiento del Problema

La empresa costarricense CORGIA Gestión e Ingeniería Alternativa, inscrita al Colegio Federado de Ingenieros y Arquitectos de Costa Rica, con más de una década en el mercado de consultorías eléctricas, se encuentra frente a desafíos que afectan su operatividad y seguridad. En este contexto, la dependencia de un servidor físico local ha generado limitaciones en el acceso remoto y la flexibilidad en el trabajo. Esto se traduce en restricciones significativas para la movilidad y dificultades en la adaptación a situaciones cambiantes, impactando directamente en la eficiencia operativa.

Otro aspecto crítico es la falta de partición de información en el servidor, permitiendo a todos los usuarios acceder a datos sensibles sin restricciones. Esta carencia en la separación de roles no solo representa un riesgo para la confidencialidad, sino que también aumenta la probabilidad de acceso no autorizado, generando potenciales consecuencias legales. La ausencia de acceso remoto y la carencia de protocolos de seguridad adecuados dificultan la implementación efectiva del teletrabajo, siendo un desafío particularmente relevante en contextos como el actual, donde la movilidad y la flexibilidad en el trabajo son esenciales. Esto podría afectar la continuidad operativa y la retención de talento.

Adicionalmente, la falta de coherencia en la configuración de seguridad de dispositivos crea disparidades significativas. Mientras algunas computadoras carecen de medidas de seguridad, otras cuentan con antivirus. Esta falta de uniformidad representa una vulnerabilidad importante, dificultando la aplicación consistente de medidas de protección y aumentando el riesgo de exposición a amenazas cibernéticas.

Por último, la empresa enfrenta la ausencia de un sistema eficiente de respaldo en la nube y recuperación de datos. La falta de copias de seguridad regulares expone a la organización a la pérdida permanente de información crítica, ya sea por fallos en el sistema, errores humanos o ataques cibernéticos, afectando la integridad y continuidad del negocio. La resolución de estos problemas requiere una estrategia integral que aborde las limitaciones en la infraestructura tecnológica, fortalezca la seguridad de la información y permita una adaptación ágil a las demandas cambiantes del entorno empresarial.

Objetivos

Objetivo General

Diseñar una Propuesta Integral de Optimización y Seguridad de la Infraestructura Tecnológica para la empresa CORGIA Gestión e Ingeniería Alternativa, basada en las normas ISO/IEC 27001, ISO/IEC 27002, COBIT, NIST SP 800-46 y Mejores Prácticas de ITIL, con el propósito de que se fortalezca la gestión de seguridad de la información y lograr la optimización de los procesos operativos.

Objetivos Específicos

- Diseñar una infraestructura que facilite el acceso seguro y remoto a la información, siguiendo los lineamientos de ISO/IEC 27001 y las prácticas recomendadas de ITIL.
- Definir roles y permisos, segmentando y restringiendo el acceso, asegurando la confidencialidad, integridad y disponibilidad de los datos, con el objetivo de que solo los usuarios autorizados accedan a información correspondiente a sus roles designados, en concordancia con las guías COBIT 19.
- Diseñar un plan para que se implemente el teletrabajo conforme a las directrices de ISO/IEC 27001 y NIST SP 800-46.
- Establecer normativas para que se logre una configuración uniforme de la seguridad en todos los dispositivos, tomando como guía las directrices de NIST SP 800-53 e ISO/IEC 27001.
- Diseñar estrategias prácticas para la realización regular de copias de seguridad de datos críticos, en concordancia con las normas ISO/IEC 27001 e ITIL.

Justificación

La investigación sobre la Propuesta Integral de Optimización y Seguridad de la Infraestructura Tecnológica en CORGIA Gestión e Ingeniería Alternativa se fundamenta en la necesidad apremiante de abordar desafíos que impactan directamente en la operación y seguridad de la empresa.

En la era actual, la transformación digital y la adopción de tecnologías modernas son cruciales. Esta propuesta busca alinear a CORGIA con las tendencias tecnológicas actuales,

facilitando una transición sin inconvenientes hacia un entorno de trabajo remoto y asegurando la continuidad operativa ante cambios inesperados. La implementación de la propuesta no sólo optimizará la infraestructura, permitiendo a los empleados acceder a la información de manera remota y segura, sino que también mejorará la eficiencia operativa, impulsando la productividad y optimizando los procesos.

El fortalecimiento de la seguridad de la información es un pilar esencial de esta investigación. La aplicación de políticas y protocolos basados en estándares internacionales no solo protege la confidencialidad de los datos, sino que también posiciona a CORGIA como una empresa comprometida con las mejores prácticas y capaz de cumplir con regulaciones internacionales de seguridad de la información. La estrategia de respaldo basada en normativas específicas garantiza la continuidad del negocio en casos de incidentes. La rápida recuperación de datos críticos minimiza el impacto de posibles pérdidas de información, asegurando la estabilidad operativa.

Finalmente, la implementación de una infraestructura tecnológica avanzada y segura posiciona a CORGIA como una empresa competitiva en el mercado, capaz de adaptarse rápidamente a las demandas cambiantes y ofrecer servicios de alta calidad en el sector de consultorías eléctricas.

Viabilidad Técnica

La viabilidad técnica de la investigación se sustenta en la consideración integral de varios aspectos que aseguran la posibilidad y éxito en el desarrollo de la propuesta. A continuación, se detallan los elementos clave que respaldan la viabilidad técnica del proyecto:

CORGIA cuenta con una infraestructura de red local (LAN) y un servidor central. La existencia de esta infraestructura establece una base sólida para la implementación de mejoras y la integración de tecnologías avanzadas. En cuanto al hardware disponible, la empresa posee 10 computadoras, entre estas el servidor central mencionado y dispositivos de almacenamiento, como discos externos con la información y documentos de la empresa. Estos recursos constituyen el hardware necesario para implementar las soluciones propuestas, como firewalls, sistemas de detección de intrusiones, y herramientas de monitoreo y auditoría.

No se requiere un espacio físico adicional para llevar a cabo la investigación. Todas las mejoras propuestas se implementarán en la infraestructura existente sin necesidad de expansión física. Se considerará la adquisición de licencias para herramientas y soluciones recomendadas, como antivirus, soluciones VPN, sistemas de seguridad de red, y herramientas de monitoreo. Esto garantizará el cumplimiento legal y la utilización de versiones actualizadas y seguras.

Referente a la capacidad de almacenamiento actual del servidor, con 327GB de espacio y un uso de 282GB, es suficiente para respaldar la implementación de medidas de seguridad y almacenar copias de seguridad de manera efectiva, con un sistema de rotación, siempre y cuando se pueda implementar las copias efectivas de almacenamiento en la nube.

La propuesta de teletrabajo se adapta a las capacidades tecnológicas actuales de la empresa. La implementación de VPN y medidas de seguridad específicas permitirá a los empleados acceder de manera segura a los recursos desde ubicaciones remotas, de la misma manera, se seleccionarán soluciones y herramientas que sean compatibles con el software actualmente utilizado por la empresa. Esto garantizará una transición sin problemas y la coexistencia de las nuevas tecnologías con las aplicaciones existentes.

Se llevará a cabo una evaluación exhaustiva de los requisitos técnicos antes de la implementación. Esto asegura que las soluciones propuestas sean escalables, eficientes y cumplan con los estándares tecnológicos requeridos.

En conjunto, estos factores demuestran la viabilidad técnica del proyecto, destacando la capacidad de integrar tecnologías avanzadas en la infraestructura existente de CORGIA Gestión e Ingeniería Alternativa, sin comprometer la operación actual y asegurando mejoras significativas en la seguridad y eficiencia de la empresa.

Viabilidad Operativa

La viabilidad operativa de la investigación se centra en la capacidad de implementar efectivamente la propuesta y garantizar su adopción exitosa por parte de los usuarios. A continuación, se detallan los aspectos que respaldan la viabilidad operativa del proyecto:

CORGIA cuenta con un equipo de 5 empleados, especializados en consultorías eléctricas. Aunque no se cuenta con un departamento dedicado a la seguridad informática, la empresa tiene la flexibilidad para contratar personal calificado o capacitar a los empleados existentes según sea necesario. Se llevará a cabo un programa de capacitación para el personal, este mismo, posterior a la finalización del trabajo de graduación como un acuerdo con la empresa, enfocado en las nuevas prácticas de seguridad, el uso de herramientas específicas y la adaptación a las nuevas tecnologías. Este entrenamiento asegurará una transición sin inconvenientes y la correcta utilización de las nuevas capacidades.

Todos los empleados de CORGIA, incluyendo aquellos que trabajan en consultorías eléctricas y administración de proyectos, serán usuarios del prototipo. Además, se capacitará a los usuarios para el acceso remoto seguro y la correcta aplicación de las medidas de seguridad, además, es importante recalcar que la implementación de medidas de seguridad y la adopción de tecnologías no están diseñadas para provocar una reducción de personal. Más bien, se centran en optimizar procesos, mejorar la seguridad y fortalecer la eficiencia operativa, lo que puede conducir a un mejor uso de los recursos humanos existentes.

La propuesta no busca cambiar fundamentalmente las tareas diarias, sino mejorar la forma en que se realizan. La introducción de medidas de seguridad y tecnologías avanzadas puede requerir ajustes en los procesos, pero el objetivo principal es facilitar y asegurar las operaciones actuales.

En resumen, la viabilidad operativa se respalda mediante la preparación y capacitación del personal, la atención a las necesidades específicas de los usuarios, y la evaluación constante para garantizar la utilidad y eficacia del sistema propuesto.

Viabilidad Económica

Dado que la investigación no implica la implementación de la propuesta, se excluye el costo de desarrollo, ya que no se realizarán gastos asociados con la contratación de especialistas o la ejecución práctica de la propuesta, sin embargo, se contemplan gastos tales como Software, este costo incluirá la adquisición de licencias para software de seguridad, herramientas de monitoreo, soluciones VPN y cualquier otra aplicación necesaria para el desarrollo del plan que se propone.

También se considerarán los costos de actualización y renovación de licencias para garantizar la validez de la propuesta a lo largo del tiempo.

Se ha mencionado la utilización del hardware actual de la empresa, sin embargo, se requiere la adquisición de algunas opciones de hardware adicionales o mejoras según las necesidades teóricas del proyecto. Esto podría abarcar algún dispositivo para convertir la infraestructura LAN actual en una opción de acceso remoto, dispositivos de seguridad de red, sistemas de respaldo y cualquier equipo necesario para respaldar la infraestructura propuesta, aunque no se implementará físicamente.

Se considerarán costos asociados con las actualizaciones teóricas de software y hardware para asegurar la sostenibilidad a largo plazo de la propuesta, finalmente, se pueden contemplar gastos imprevistos, como costos de consultoría teórica, y cualquier otro gasto no contemplado anteriormente, aunque no se materializarán en la implementación.

Esta estructura de costos respalda la viabilidad económica de la investigación, permitiendo un análisis teórico del retorno de inversión (ROI) en términos de beneficios operativos y de seguridad, sin incurrir en gastos asociados con la ejecución práctica de la propuesta.

Software de Seguridad

Para abordar de manera efectiva la seguridad informática en cualquier entorno organizacional, es esencial comprender las diferentes opciones disponibles en términos de licencias de software, hardware y servicios especializados. En este contexto, las tablas presentadas a continuación ofrecen una visión detallada de las diversas alternativas disponibles en el mercado para fortalecer la infraestructura y proteger los activos de información de una empresa.

Tabla 1

Licencias de Antivirus

Dispositivo	Precio	Regularidad de Pago	Características Principales
AGV Security	$60	Anual	Protección antivirus avanzada, protección contra ransomware, firewall, protección de webcam, anti-phishing, optimización del sistema, VPN segura, AntiTrack
McAfee Endpoint Security	$36	Anual	Protección antivirus, protección contra ransomware, firewall, detección de intrusos, seguridad de la red, administración centralizada
Norton Antivirus	$65	Anual	Protección antivirus, protección contra ransomware, firewall, protección de identidad en línea, protección de transacciones financieras, administración remota

Fuente: Elaboración Propia, 2024

Después de presentar la tabla de licencias de antivirus, es importante contextualizar la siguiente tabla sobre licencias de Software. Se presentan Softwares que cumplen distintas funciones, entre los principales los de herramientas en la nube como Office, Google y Zoho que pasarán a desempeñar el papel principal de infraestructura. Así como el software de monitoreo que se estará implementando y la solución VPN para controlar los accesos permitidos desde la red como si esta fuese la misma red local que poseen actualmente.

Tabla 2

Licencias de Software de Monitoreo

Dispositivo	Precio	Regularidad de Pago	Características Principales
SolarWinds Network Performance Monitor	$1,800	Única vez	Monitoreo de red avanzado, análisis de rendimiento, alertas en tiempo real
PRTG Network Monitor	$1500 - $1700	Única vez por licencia	Monitore de red y sistemas, paneles personalizables, alertas flexibles
Nagios	Gratis	NA	Monitoreo de infraestructura de TI, gestión de incidentes, alertas y notificaciones

Fuente: Elaboración Propia, 2024

Continuando con la temática de seguridad digital, la siguiente tabla presenta soluciones VPN, un componente esencial para garantizar conexiones seguras y confiables en entornos remotos o distribuidos. Las opciones de VPN presentadas abordan diferentes necesidades y modelos de pago, lo que permite una adaptación a las exigencias específicas de cada organización.

Tabla 3

Soluciones VPN

Dispositivo	Precio	Regularidad de Pago	Características Principales
Cisco AnyConnect	$173	5 años 25 usuarios	Soporta IPSec, cifrado avanzado, autenticación multifactor, fácil de implementar
OpenVPN	$75	Mensual	Código abierto, soporte para múltiples plataformas, cifrado fuerte, adaptable
WatchGuard UTM	$365	Anual	Soporte Ipsec, cifrado, seguridad web, antivirus, control de aplicaciones, visibilidad en la red

Fuente: Elaboración Propia, 2024

Luego de explorar las opciones de seguridad en la red y monitoreo, es crucial dirigir la atención hacia las necesidades de actualización de software, un aspecto fundamental en la gestión de la seguridad informática en cualquier empresa. La actualización periódica del software es un componente esencial para mantener la integridad y la seguridad de los sistemas y aplicaciones en el entorno empresarial. Con cada actualización, se implementan parches de seguridad y correcciones de errores que ayudan a mitigar vulnerabilidades potenciales y a fortalecer la resistencia de los sistemas ante posibles amenazas cibernéticas.

Tabla 4

Office 365

Dispositivo	Precio	Regularidad de Pago	Características Principales
Business Basic	$6 c/usuario	Mensual	Correo electrónico, OneDrive (1 TB), Teams, SharePoint, Word, Excel, PowerPoint (web y móvil)
Business Standard	$12.50 c/usuario	Mensual	Todo en Business Basic, además de aplicaciones de Office completas para escritorio, Microsoft Bookings
Business Premium	$22 c/usuario	Mensual	Todo en Business Standard, además de funcionalidades avanzadas de seguridad y gestión de dispositivos, Intune, Azure Information Protection

Fuente: Elaboración Propia, 2024

Office 365 es de los paquetes de tecnología en la nube más conocido y utilizado alrededor del mundo, esto se debe a la robustez y trayectoria que han demostrado a lo largo de los años, así como garantizar la calidad de los servicios que proveen en una excelente relación precio – calidad. Sin embargo, no son los únicos competentes en el mercado, a continuación, se enlistan otras opciones a considerar para la propuesta.

Tabla 5

Google Workspace

Dispositivo	Precio	Regularidad de Pago	Características Principales
Business Starter	$6 c/usuario	Mensual	Correo electrónico, Google Drive (30 GB), Google Meet, Docs, Sheets, Slides
Business Standard	$12 c/usuario	Mensual	Todo en Business Starter, además de Google Drive con 2 TB, Google Meet grabaciones, Seguridad y administración avanzada
Business Plus	$18 c/usuario	Mensual	Todo en Business Standard, además de funcionalidades avanzadas de seguridad y gestión de dispositivos, Intune, Azure Information Protection

Fuente: Elaboración Propia, 2024

De la misma manera se enfrenta en este mismo mercado de las tecnologías en la nube, la tecnología de Zoho, ofrece paquetes con la misma prestación de servicios al igual que office y Google que son considerados los mejor posicionados en este mercado.

Tabla 6

Zoho Workplace

Dispositivo	Precio	Regularidad de Pago	Características Principales
Standard	$3 c/usuario	Mensual	Correo electrónico, Zoho Docs (30 GB), Zoho Office Suite, Zoho Cliq, Zoho Connect
Professional	$6 c/usuario	Mensual	Todo en Standard, además de Zoho Docs con 100 GB, Zoho ShowTime, Zoho Meeting, Zoho WorkDrive

Fuente: Elaboración Propia, 2024

Finalmente, se presenta información sobre consultores independientes en seguridad informática. Estos profesionales pueden ofrecer asesoramiento especializado y servicios personalizados para fortalecer la postura de seguridad de una organización frente a las amenazas cibernéticas.

Tabla 7

Consultores independientes en seguridad informática

Motivo	Precio	Regularidad de Pago
Honorarios Profesionales	CRC 15.613,91	Por Hora

Fuente: Elaboración Propia, 2024

Viabilidad Legal

Se asume que la implementación teórica de la propuesta cumple con las leyes y regulaciones vigentes en Costa Rica en materia de seguridad informática y protección de datos. Limitaciones pueden surgir si existen cambios en la legislación durante el desarrollo de la investigación.

En referencia al modo de operación de la organización, esta opera actualmente con una infraestructura que almacena información en un servidor local. El acceso a la información se realiza internamente, generando restricciones significativas. La propuesta busca mejorar esta situación, pero se deben considerar las leyes y regulaciones existentes.

Los requisitos incluyen el cumplimiento de las leyes de protección de datos, seguridad informática y derechos de autor en el ámbito tecnológico. La propuesta deberá respetar y adherirse a la legislación costarricense aplicable.

Se evaluarán distintas alternativas para garantizar el cumplimiento legal, considerando tecnologías y prácticas que se alineen con las leyes: Ley 8148 Adición de los artículos 196 BIS, 217 BIS y 229 BIS al Código Penal, Ley N°4573 para reprimir y sancionar los delitos informáticos de la Asamblea Legislativa de la República de Costa Rica del año 2001, Ley de Derechos de Autor 6683 por parte de la Asamblea Legislativa de la República de Costa Rica del año 1982, Ley 8968 sobre la protección de la persona frente al tratamiento de sus datos personales. Las oportunidades residirán en el fortalecimiento de la seguridad de la información y la protección de datos personales, contribuyendo al cumplimiento legal de CORGIA.

Proyecciones

La investigación busca proporcionar a CORGIA Gestión e Ingeniería Alternativa una Propuesta Integral de Optimización y Seguridad de la Infraestructura Tecnológica que permita fortalecer la gestión de seguridad de la información y optimizar los procesos operativos. Se espera que la implementación de esta propuesta resulte en una infraestructura tecnológica robusta, segura y eficiente, adaptada a las mejores prácticas internacionales. Tratando de preservar la infraestructura actual que sea funcional y que pueda adaptarse a la propuesta en estudio para alcanzar los objetivos propuestos.

La implementación de la Propuesta Integral de Optimización y Seguridad de la Infraestructura Tecnológica conlleva beneficios significativos para CORGIA Gestión e Ingeniería Alternativa. En primer lugar, se garantiza una mejora sustancial en la seguridad de la información mediante la aplicación de políticas y protocolos que resguardan la confidencialidad, integridad y disponibilidad de los datos, reduciendo así la exposición a amenazas cibernéticas. Además, se prevé una optimización palpable de los procesos operativos, especialmente en el contexto del trabajo remoto, lo que contribuirá a una mayor eficiencia y productividad, facilitando la adaptación a situaciones cambiantes.

Asimismo, se fortalecerá la postura de la organización frente a vulnerabilidades y amenazas cibernéticas mediante la implementación de estándares de seguridad en todos los dispositivos. La garantía de continuidad del negocio se verá respaldada por estrategias eficientes de respaldo de datos, asegurando una pronta recuperación en caso de incidentes. Por último, la cultura de seguridad se verá mejorada con programas de capacitación y concientización, asegurando que el personal esté debidamente formado y consciente de la importancia de seguir prácticas seguras en el entorno tecnológico.

Alcance Funcional

En el ámbito de la seguridad informática y la gestión de recursos tecnológicos, el alcance funcional establece los parámetros esenciales que guían la implementación efectiva de medidas de seguridad y operatividad en un entorno empresarial digitalizado. Este concepto abarca una serie de áreas críticas que se centran en garantizar la integridad, confidencialidad y disponibilidad de los datos, fundamentales para el éxito operativo y la protección de los activos de información.

Dentro de este contexto, el alcance funcional comprende diversas dimensiones, cada una dirigida a abordar aspectos específicos de la seguridad y el rendimiento tecnológico. Desde el acceso remoto y seguro hasta la gestión de copias de seguridad, cada área representa un pilar fundamental en la estructura de seguridad de una organización, delineando políticas, protocolos y procedimientos que aseguran la protección y disponibilidad de los datos críticos.

Acceso Remoto y Seguro: Plan de implementación de una infraestructura avanzada que permita el acceso remoto a la información de manera segura. Utilización de redes virtuales privadas (VPN) como opción principal para asegurar la confidencialidad e integridad de los datos durante las conexiones remotas. Configuración de medidas de autenticación robustas para garantizar la identidad de los usuarios que acceden de forma remota.

Gestión de Seguridad de la Información: Definición detallada de políticas de seguridad de la información, alineadas con normas ISO/IEC 27001, ISO/IEC 27002 y COBIT. Establecimiento de roles y permisos específicos para cada usuario, garantizando un acceso controlado y seguro a la información. Implementación de protocolos que aseguren la disponibilidad de los datos, fortaleciendo así la confidencialidad e integridad de la información.

Teletrabajo Eficiente: Desarrollo de un plan integral para la implementación efectiva del teletrabajo basado en ISO/IEC 27018 y NIST SP 800-46. Reforzamiento de la autenticación con tecnologías avanzadas, implementación de encriptación para la protección de datos sensibles y establecimiento de un sistema de monitoreo de actividades para garantizar la seguridad durante el trabajo remoto. Adopción de medidas para asegurar la conectividad segura y eficiente de los empleados desde ubicaciones remotas.

Configuración Uniforme de la Seguridad: Establecimiento de estándares de seguridad basados en NIST SP 800-53 e ISO/IEC 27001 para lograr una configuración uniforme en todos los dispositivos. Definición de procedimientos y políticas para la instalación de antivirus, configuraciones de cortafuegos y otras medidas esenciales en todos los dispositivos. Garantía de coherencia y robustez en la defensa contra amenazas cibernéticas mediante la aplicación sistemática de los estándares de seguridad definidos.

Gestión de copias de seguridad: Desarrollo de estrategias sólidas basadas en normas ISO/IEC 27031 e ITIL para la realización periódica y automatizada de copias de seguridad de datos críticos. Implementación de segmentación eficiente de datos según su importancia y la creación de procedimientos de prueba para validar la efectividad de los respaldos. Diseño de un plan estratégico que simplifique la aplicación de estas normas en la infraestructura organizacional futura, dejando la capacitación del personal y la concientización para garantizar la adhesión efectiva al modelo propuesto como un acuerdo entre la empresa y el estudiante posterior al proyecto de graduación.

Tabla 8

Propuesta de Optimización y Seguridad de la Infraestructura Tecnológica de la Empresa Corgia Gestión e Ingeniería

Nombre del apartado	Descripción del apartado
Infraestructura de Acceso y Gestión de Datos.	Este apartado se centrará en diseñar una infraestructura que facilite el acceso a la información de manera remota y segura, siguiendo los lineamientos de ISO/IEC 27001 y las prácticas recomendadas de ITIL. Se elaborará políticas y protocolos de seguridad, referenciados en las normas ISO/IEC 27001, que regulen el acceso a los datos y asegure confidencialidad, considerando redes virtuales privadas (VPN) como primera opción de solución. La propuesta realizará un comparativo respaldado por políticas y protocolos, que puedan integrarse en el entorno actual, permitiendo el acceso remoto sin comprometer la seguridad de la información.
Planificación de Implementación de Políticas de Seguridad	Este apartado se fundamentará en las mejores prácticas definidas en ISO/IEC 27002 y las pautas de COBIT, se elaborará una propuesta que detalle las fases para incorporar estas políticas en la infraestructura empresarial actual, definiendo roles y permisos para salvaguardar la confidencialidad, integridad y disponibilidad de los datos. Se logrará mediante la segmentación y restricción de acceso, garantizando que únicamente los usuarios autorizados accedan a la información correspondiente a sus roles designados.
Desarrollo de Teletrabajo y Protocolos de Seguridad	Este apartado tiene como fin primordial redactar una propuesta que permita implementar el teletrabajo mediante soluciones basadas en las directrices de ISO/IEC 27018 y

Nombre del apartado	Descripción del apartado
Infraestructura de Acceso y Gestión de Datos.	Este apartado se centrará en diseñar una infraestructura que facilite el acceso a la información de manera remota y segura, siguiendo los lineamientos de ISO/IEC 27001 y las prácticas recomendadas de ITIL. Se elaborará políticas y protocolos de seguridad, referenciados en las normas ISO/IEC 27001, que regulen el acceso a los datos y asegure confidencialidad, considerando redes virtuales privadas (VPN) como primera opción de solución. La propuesta realizará un comparativo respaldado por políticas y protocolos, que puedan integrarse en el entorno actual, permitiendo el acceso remoto sin comprometer la seguridad de la información.
	NIST SP 800-46. Se diseñará un plan con las etapas que se deben concretar para implementar los protocolos de seguridad que refuercen la autenticación, encriptación y monitoreo de actividades. Este plan abarcará las herramientas y tecnologías que mejor se adapten a la infraestructura existente para lograr una implementación segura, que resulte en una optimización integral de los procesos operativos en consonancia con las mejores prácticas internacionales.
Estandarización en la Configuración de Seguridad	Este apartado busca establecer normativas para lograr una configuración uniforme de la seguridad en todos los dispositivos, tomando como guía las directrices de NIST SP 800-53 e ISO/IEC 27001. Se definirán estándares que aborden la instalación de antivirus, configuraciones de cortafuegos y otras medidas esenciales. La propuesta se centrará en la creación de un plan de implementación de los estándares para asegurar coherencia y robustez en la defensa contra amenazas

Nombre del apartado	Descripción del apartado
Infraestructura de Acceso y Gestión de Datos.	Este apartado se centrará en diseñar una infraestructura que facilite el acceso a la información de manera remota y segura, siguiendo los lineamientos de ISO/IEC 27001 y las prácticas recomendadas de ITIL. Se elaborará políticas y protocolos de seguridad, referenciados en las normas ISO/IEC 27001, que regulen el acceso a los datos y asegure confidencialidad, considerando redes virtuales privadas (VPN) como primera opción de solución. La propuesta realizará un comparativo respaldado por políticas y protocolos, que puedan integrarse en el entorno actual, permitiendo el acceso remoto sin comprometer la seguridad de la información.
	cibernéticas, fortaleciendo la postura de la organización frente a posibles vulnerabilidades.
Plan de Implementación de Estrategias de Respaldo y Recuperación	Este apartado se centra en diseñar estrategias prácticas para la realización regular de copias de seguridad de datos críticos, en concordancia con las normas ISO/IEC 27031 e ITIL. El enfoque estará dirigido en la creación de un plan estratégico que simplifique la aplicación de las normas en la infraestructura organizacional futura, mediante la automatización del proceso de respaldo, la segmentación eficiente de datos según su importancia y el establecimiento de procedimientos de prueba para validar la eficacia de los respaldos. La estrategia incluye un plan de capacitación del recurso humano y la concientización para garantizar una adhesión efectiva al modelo propuesto.

Fuente: Elaboración Propia, 2024

Alcance Metodológico

Se adoptará un enfoque metodológico centrado en la planificación detallada y estratégica, excluyendo la implementación práctica y el monitoreo de resultados debido a limitaciones temporales. El proceso se llevará a cabo en las siguientes fases:

Análisis de Requerimientos**:** Identificación exhaustiva de las necesidades específicas de seguridad y operativas de CORGIA Gestión e Ingeniería Alternativa. Realización de entrevistas con los *stakeholders* para comprender a fondo las expectativas y requisitos de seguridad, así como los desafíos operativos existentes. Documentación detallada de los hallazgos, definiendo claramente los objetivos a alcanzar durante la investigación.

Diseño Detallado: Elaboración minuciosa de la propuesta detallada, abarcando políticas, protocolos y procedimientos específicos para cada componente de la infraestructura. Integración de normas ISO/IEC 27001, ISO/IEC 27002, COBIT, NIST SP 800-46 y Mejores Prácticas de ITIL en el diseño, garantizando la alineación con estándares internacionales reconocidos. Desarrollo de documentación detallada que sirva como guía para la implementación futura.

Desarrollo de Estrategias de Implementación: Diseño de estrategias detalladas para la construcción e implementación gradual de las soluciones propuestas. Establecimiento de etapas y fases claras para la ejecución de las estrategias, priorizando los aspectos críticos de seguridad y acceso remoto.

Elaboración de Programas de Capacitación y Concientización: Desarrollo de programas detallados de capacitación y concientización dirigidos al personal de CORGIA. Creación de material didáctico, sesiones formativas y actividades interactivas para asegurar la comprensión de los nuevos procedimientos y políticas de seguridad, esto como acuerdo posterior a la finalización del proyecto de graduación.

Alcance Tecnológico

Considerando la necesidad de modernizar la infraestructura para facilitar el teletrabajo, se propone una serie de tecnologías y soluciones que permitirán a CORGIA Gestión e Ingeniería Alternativa mejorar su eficiencia y seguridad:

De acuerdo con la infraestructura de Red Moderna, se sugiere la implementación de una red basada en la nube para facilitar el acceso remoto. Soluciones como Cisco Meraki o Aruba *Instant On* proporcionan una gestión centralizada y acceso seguro desde cualquier ubicación. Para herramientas de Colaboración en la Nube, es necesaria la adopción de plataformas de colaboración en la nube. Microsoft Teams o Slack permiten la comunicación efectiva, compartir documentos y colaboración en tiempo real.

Para la Autenticación Multifactorial (MFA por sus siglas en inglés) se da un reforzamiento de la seguridad mediante la implementación de la autenticación multi factor. Google Workspace o Microsoft 365 ofrecen opciones de MFA para proteger el acceso a las cuentas, y la utilización de una VPN segura para garantizar el acceso remoto de manera protegida. *NordVPN for Business* o *Cisco AnyConnect* son opciones confiables para establecer conexiones seguras, esta segunda es compatible con la infraestructura Meraki y Aruba, y puede configurarse para establecer una conexión segura con la red.

Se considera una transición hacia un sistema de almacenamiento más moderno como lo es en la nube y no precisamente local que, depende de un entorno físicos. Google Drive for Business o Dropbox Business permite acceder y compartir archivos de manera segura desde cualquier lugar. Relacionado a la gestión de dispositivos y seguridad *endpoint*, es requerida la implementación de soluciones para estos, por ejemplo, Microsoft Intune o VMware Workspace ONE facilitan la administración remota y garantizan la seguridad de estos.

Finalmente, la utilización de un firewall en la nube para proteger el tráfico entrante y saliente es crucial para Corgia, esto con la intención de protegerse y ofrecer proactividad ante posibles ataques cibernéticos. Soluciones como *Cloudflare* o *AWS WAF* brindan seguridad robusta sin comprometer la velocidad.

Teniendo en cuenta la infraestructura actual, se sugiere una evaluación y actualización de dispositivos, para esto es necesario verificar la compatibilidad de las computadoras actuales con la transición a un entorno de trabajo remoto y considerar la actualización de hardware si es necesario. Establecer políticas de seguridad claras y configurar permisos de acceso según roles definidos en la red y en la nube. Y proporcionar capacitación detallada sobre el uso de las nuevas

herramientas y prácticas de seguridad a los empleados, para conocer y sacar provecho máximo de las nuevas implementaciones.

CAPÍTULO II: MARCO REFERENCIAL

CORGIA Gestión e Ingeniería Alternativa es una empresa costarricense enfocada en el área eléctrica, que ofrece servicios profesionales de consultoría, diseño e inspección eléctrica, así como la elaboración de estudios de potencia para instalaciones de energía eléctrica, administración y dirección de proyectos eléctricos, se encuentra inscrita al Colegio Federado de Ingenieros y Arquitectos de Costa Rica, que según La Junta Directiva General conformada para el periodo del 7 de Noviembre 2023 al 31 de Octubre 2024, su misión es (CFIA, 2023) "Asegurar la excelencia y el decoro de los miembros, para el desarrollo de un ejercicio profesional eficiente, responsable e interdisciplinario de las ingenierías y de la arquitectura, para coadyuvar con la seguridad y el progreso sostenible del país." (párr. 1)

CORGIA actualmente cuenta con una infraestructura limitada en hardware, que es la parte física de un sistema informático, de la que disponen únicamente de 10 computadoras, entre estas un único servidor físico local, que es un equipo que está instalado físicamente en la misma ubicación que los dispositivos que se vinculan con dicho servidor, en este caso en las instalaciones de CORGIA. Estos dispositivos acceden a la información ubicada en este Servidor Físico Local mediante una Red de Área Local o bien, red LAN, por sus siglas, que según (Cisco Networking, 2019), conecta equipos informáticos ubicados en un área geográfica reducida, como un edificio o una habitación, esta característica específica de la infraestructura actual de la empresa impide el acceso remoto, que consiste en acceder a los datos que se almacenan en este servidor a distancia, sin requerir una conexión en el mismo entorno, si no, a través de una red virtual.

Generalidades

A través de esta investigación, se busca mejorar esta infraestructura y definir un plan que permita modificarla para incluir otras tecnologías que eventualmente le permitan a la empresa CORGIA realizar teletrabajo, que según la Universidad Estatal a Distancia en su artículo de Programa de Teletrabajo (UNED, 2019):

> El teletrabajo se fundamenta en el uso intensivo de internet y de las tecnologías de la información y comunicación (TIC) para llevar a cabo tareas, asignaciones o proyectos desde el lugar y el horario que así convenga el colaborador junto con su empresa. (párr. 1)

Y con esto garantizar que la información y herramientas que los colaboradores requieran para realizar sus tareas pueda ser accesible desde cualquier otro lugar fuera de las instalaciones físicas de la empresa, cumpliendo a cabalidad con la Ley N.º 9738 Ley Para Regular El Teletrabajo establecida en la Gaceta en Costa Rica. (La Gaceta, 2019).

La optimización de la infraestructura tecnológica en CORGIA Gestión e Ingeniería Alternativa implica la consideración de conceptos fundamentales, siendo la segmentación de roles uno de ellos. Este enfoque estratégico implica asignar funciones y responsabilidades específicas a cada miembro del equipo, asegurando que el acceso a la información esté delimitado por las tareas y necesidades particulares de cada individuo. En el contexto de esta investigación, la segmentación de roles se erige como un pilar esencial para fortalecer la seguridad de los datos y optimizar la eficiencia operativa, permitiendo que cada colaborador acceda solo a la información relevante para su labor específica.

En paralelo, el concepto de acceso a la información toma relevancia al considerar la implementación de tecnologías como las *VPN* (Redes Virtuales Privadas). Este aspecto crucial permitirá no solo un acceso remoto seguro a los datos almacenados en el servidor físico local, sino que también posibilitará a los colaboradores acceder a la información esencial desde cualquier ubicación externa, como se mencionaba anteriormente. La integración de estas tecnologías se alinea con la necesidad de adaptabilidad y flexibilidad en el entorno laboral actual, promoviendo un modelo de trabajo que responde a las demandas cambiantes.

Asimismo, en el marco de la seguridad de la información, es imperativo abordar la noción de datos sensibles. Estos datos, que pueden incluir información personal, financiera o estratégica, requieren una atención especial en términos de confidencialidad y manejo seguro. La propuesta integral contempla políticas y protocolos basados en normativas y estándares internacionales, como ISO/IEC 27001, para asegurar la protección de estos datos sensibles y cumplir con las regulaciones, incluyendo la Ley N.º 8968 sobre la protección de datos personales en Costa Rica.

La inexistencia de protocolos de seguridad en la infraestructura actual de CORGIA Gestión e Ingeniería Alternativa plantea un desafío significativo en la protección de sus activos de información. Los protocolos de seguridad, que comprenden políticas y procedimientos, son

esenciales para salvaguardar la confidencialidad, integridad y disponibilidad de los datos (Mattord, 2016). La falta de tales protocolos deja a la organización vulnerable a amenazas cibernéticas, resaltando la necesidad urgente de implementar medidas basadas en normativas reconocidas, como ISO/IEC 27001, para establecer un marco de seguridad robusto y eficaz. En el ámbito de la seguridad de dispositivos, la disparidad en la configuración de las computadoras de la empresa implica una debilidad potencial. La homogeneización de la seguridad informática se vuelve imperativa para garantizar una defensa uniforme contra amenazas (Dhillon & Moores, 2001). La implementación de soluciones antivirus uniformes, como AVG Internet Security en todas las máquinas, no solo protegerá contra malware conocido, sino que también mitigará el riesgo de nuevas amenazas.

La incorporación de un software antivirus es esencial para contrarrestar las crecientes amenazas cibernéticas. “Los antivirus detectan y eliminan software malicioso, protegiendo los sistemas contra intrusiones.” (Pfleeger & Pfleeger, 2012, págs. 223-225) La actualización regular y la estandarización de soluciones antivirus, como AVG TuneUp, son prácticas recomendadas para mantener una línea de defensa eficiente y actualizada contra amenazas en constante evolución.

Las amenazas cibernéticas constituyen un conjunto diverso de acciones mal intencionadas dirigidas a comprometer la seguridad y la integridad de la información en entornos digitales. Estas amenazas abarcan una amplia gama de actividades perjudiciales que buscan explotar vulnerabilidades en sistemas informáticos y redes. Un componente clave de las amenazas cibernéticas es el phishing, que implica la utilización de tácticas engañosas, como correos electrónicos fraudulentos o sitios web falsos, para obtener información confidencial, como contraseñas o datos financieros.

Otra forma común de amenaza cibernética es el malware, que engloba software malicioso diseñado para dañar o acceder a sistemas informáticos sin autorización. Ejemplos de malware incluye virus, gusanos, troyanos y *ransomware*, cada uno con objetivos específicos que van desde la destrucción de datos hasta la extorsión económica.

Las vulnerabilidades en la red representan otra categoría de amenazas cibernéticas, refiriéndose a debilidades en la infraestructura de red que podrían ser explotadas para obtener

acceso no autorizado a sistemas o información confidencial. Estas vulnerabilidades pueden surgir de configuraciones incorrectas, falta de actualizaciones de seguridad o deficiencias en el diseño de la red. En este contexto, la implementación de medidas de seguridad como firewalls y sistemas de detección de intrusiones se vuelve esencial. Los firewalls actúan como barreras protectoras, monitoreando y controlando el tráfico de red para prevenir accesos no autorizados. Por otro lado, los sistemas de detección de intrusiones analizan patrones de tráfico y comportamientos inusuales para identificar posibles amenazas y tomar medidas correctivas.

La carencia de un sistema de respaldo adecuado expone a CORGIA al riesgo de pérdida de datos críticos. Un sistema de respaldo se refiere a un conjunto de procesos y tecnologías diseñados para copiar y almacenar información crítica con el objetivo de asegurar su disponibilidad y recuperación en caso de pérdida, ya sea debido a fallos del sistema, errores humanos, desastres naturales o ataques cibernéticos (Whitman & Mattord, 2016). En esencia, funciona como un mecanismo de seguro para resguardar datos valiosos y garantizar la continuidad del negocio.

La implementación de un sistema automatizado de respaldo implica la utilización de herramientas y software especializado que realiza copias periódicas y programadas de los datos, asegurando que la información más reciente esté siempre respaldada y lista para ser recuperada en caso de necesidad. Esto no solo protege contra la pérdida de datos, sino que también facilita la rápida restauración de la información a su estado original.

Soluciones en la Nube

Por otro lado, la nube es un paradigma tecnológico que permite el almacenamiento y acceso a datos y servicios a través de internet, en lugar de depender exclusivamente de recursos locales. En el contexto de la informática, un sistema de respaldo en la nube implica utilizar servicios de almacenamiento remoto para respaldar y recuperar datos. Plataformas como Google Drive o Dropbox son ejemplos de servicios en la nube que ofrecen capacidades de respaldo automático y acceso remoto a la información respaldada.

Ventajas de la nube

Inicialmente, una de sus principales ventajas es la comodidad que se ofrece a los usuarios, ya que las copias de seguridad locales conllevan a tediosas tareas manuales que requieren de tiempo y recursos. Por otro lado, es más difícil controlar el progreso, o solucionar algún inconveniente, los servicios de respaldo en la nube, generalmente se encargan automáticamente de realizar tareas como estas lo que resulta beneficioso para el usuario de enfocarse en otras tareas e incrementar su productividad.

El respaldo en la nube no solo proporciona redundancia y seguridad, sino que también ofrece escalabilidad y flexibilidad. En cuanto a redundancia, la misma se garantiza ya que esta copia de seguridad existirá con redundancia geográfica y por zonas, los datos no son únicamente fáciles de recuperar cuando se necesiten sino que también se encuentran protegidos contra desastres o daños irreparables, esto se debe a que las copias de seguridad se guardan en un sistema remoto, finalmente la protección de datos se debe a que se mitigan los problemas ocasionados por errores humanos como la eliminación accidental de algún archivo. Generalmente, la copia de seguridad en la nube se cifra antes de enviarse al servidor en la que se almacenará, esto contribuye a que usuarios no autorizados accedan a los datos mientras la copia de seguridad está en curso o una vez completada, por lo que los datos permanecen seguros e íntegros, aunque sean interceptados durante su transferencia.

La escalabilidad permite adaptar la capacidad de almacenamiento según las necesidades de la empresa, lo que es beneficioso ya que se pueden realizar copias de seguridad de los datos que se deseen, el servicio se adaptará a medida que se amplíen los requisitos de capacidad y demanda, en otras palabras, se paga por lo que se utiliza. Mientras que la flexibilidad en conjunto con la accesibilidad permite acceder a los datos desde cualquier ubicación con conexión a internet, en cualquier momento que se requiera. Esta combinación de características convierte al respaldo en la nube en una solución moderna y efectiva para garantizar la integridad y disponibilidad de los datos empresariales.

Pasos para realizar un respaldo en la nube

Inicialmente se recomida investigar sobre los diferentes proveedores de este servicio que compiten en el mercado actual y las distintas opciones que ofrecen, o bien, contratar los servicios de un profesional que nos pueda brindar la asesoría necesaria para realizar dicha elección. Una vez con este conocimiento, se debe seleccionar el proveedor de servicios de respaldo en la nube, dicha elección dependerá de aspectos como el nivel de seguridad que ofrece, accesibilidad a la información con varios factores de autenticación, cifrado de la información, arquitectura del centro de datos, la tecnología que se utiliza, velocidad de carga y descarga que se ofrece, entre otras.

Seguidamente, evaluar cuáles documentos deben respaldarse, si los documentos que se someterán al sistema de respaldo contienen información sensible, para asegurarse que el proveedor cumpla con los pasos de autenticación y perfiles para acceder a la información. Una evaluación acertada para clasificar esta información es evaluar el riesgo y las medidas de seguridad que se deben contemplar para proteger esa información, para esto se le debe asignar una prioridad a los documentos que clasifiquen la información confidencial y crucial para el funcionamiento de la empresa de la no tan relevante, esto para al momento de respaldar, actuar en consecuencia. También es importante determinar si la copia de seguridad debe ser completa o parcial, generalmente los servicios de respaldo incrementan su costo a partir de cierto volumen de información, lo que provoca que respaldar información de manera indiscriminada sea ineficiente e innecesario por lo que nuevamente, es importante identificar los criterios bajo los que se clasificará la información a respaldar. En caso de ser necesario respaldar la información en su totalidad, será importante considerar algún plan de tipo anual con el proveedor.

Es recomendable tomar ventaja de los periodos de prueba de los proveedores, ya que nos permite conocer y evaluar aspectos como la interfaz que ofrece, que tan amistoso es con el usuario, la velocidad de carga y descarga, las opciones de seguridad, la posibilidad de creación y asignación de roles y permisos a los distintos usuarios, para separar el nivel de accesibilidad a la información, qué tan detallados son los informes de seguridad, el historial de actividad entre otros aspectos relevantes para una auditoría en caso de una posible actividad indeseada o desastre.

La implementación de un sistema automatizado de respaldo, basado en las mejores prácticas de la industria, será crucial para preservar la continuidad del negocio. La adopción de un sistema de respaldo en la nube ofrece una solución moderna y segura para almacenar datos de forma remota (Pearson, 2013). Plataformas como Google Drive o Dropbox permiten realizar respaldos automáticos y acceder a los datos desde cualquier ubicación. La nube ofrece todas estas comodidades y ventajas sobre un respaldo local, para satisfacer las necesidades cambiantes de la empresa.

Normas y Regulaciones Internacionales

Norma ISO 27001 / ISO 27002

En este contexto, las Normas ISO/IEC 27001 emergen como referencia primordial. Estos estándares internacionales, focalizados en la seguridad de la información, no solo establecen requisitos, sino que configuran un marco estructurado que incorpora principios esenciales como confidencialidad, integridad y disponibilidad. Este enfoque, lejos de ser ornamental, fortalece de manera tangible la seguridad, sentando las bases para el crecimiento sostenible de la organización. Con el fin de preservar la información, se ha demostrado anteriormente que no es suficiente con la implantación de controles y procedimientos de seguridad que se realizan con frecuencia, pero sin un criterio en común establecido y todo esto sin considerar toda la información esencial que se debe proteger.

Finalmente, es por esto que la Organización Internacional de Estandarización, por sus siglas ISO, ha establecido una implementación efectiva de la seguridad de la información que se desarrolla en las normas ISO 27001 y la ISO 27002 que contribuyen a un sistema de gestión de seguridad de la información o por sus siglas SGSI, estas normas consisten en medidas que están enfocadas en proteger la información, sin importar su formato, contra cualquier tipo de amenaza que pueda enfrentar, con la finalidad de garantizar la continuidad de las actividades habituales de la empresa.

La resiliencia empresarial, entendida como la capacidad de una organización para anticipar, responder y adaptarse a eventos disruptivos, se integra como un objetivo clave en el proceso de

optimización y seguridad. La norma ISO 22301, centrada en la gestión de la continuidad del negocio, se convierte en una guía para la empresa Corgia hacia la construcción de un entorno empresarial robusto y resistente. La resiliencia, en este contexto, no solo se trata de resistir a las amenazas, sino de prosperar en un mundo digital en constante cambio. Es por esto que es crucial la Seguridad de la Información, que según (Microsoft, 2024):

> La seguridad de la información, que suele abreviarse como InfoSec, es un conjunto de procedimientos y herramientas de seguridad que protegen ampliamente la información confidencial de la empresa frente al uso indebido, acceso no autorizado, interrupción o destrucción. InfoSec comprende la seguridad física y del entorno, el control de acceso y la ciberseguridad. (párr.1)

Que, a su vez, este término es en lo que se basa la norma ISO/IEC 27001, la Organización Internacional de Estandarización (ISO) a través de estas normas, busca establecer una implementación efectiva de la seguridad de la información en la empresa, lográndolo a través de esta norma y la ISO 27002 también. Según (NormasISO, 2005):

> Los requisitos de la Norma ISO 27001 norma nos aportan un Sistema de Gestión de la Seguridad de la Información (SGSI), consistente en medidas orientadas a proteger la información, indistintamente del formato de esta, contra cualquier amenaza, de forma que garanticemos en todo momento la continuidad de las actividades de la empresa. (párr.3)

Y para complementar esta norma, existe la ISO/IEC 2007 que según (NOATICA, 2023) es una guía que establece las mejores prácticas en seguridad de la información y define los requisitos para establecer, implementar, mantener y mejorar un SGSI. “Mientras que la ISO 27001 se enfoca en la estructura del SGSI, la ISO 27002 se centra en proporcionar un conjunto detallado de controles y medidas para proteger la información y mitigar riesgos específicos.” (párr.2)

En ambas normas mencionadas en los párrafos anteriores se menciona el SGSI o bien Sistema de Gestión de Seguridad de la Información, por lo que es importante reconocer el término de las Normativas de Seguridad, que según (Ministerio de Trabajo y Seguridad Social, 2020):

> El Ministerio de Trabajo y Seguridad Social reconoce la importancia de los activos de información como pilar fundamental para el correcto funcionamiento y desarrollo de los procesos institucionales.
>
> Estos activos están expuestos a riesgos, cuya materialización podría impactar en forma negativa la atención a los usuarios, por ello, es prioritario para la Administración Superior gestionar en forma adecuada la seguridad de la información con el objetivo de minimizar la exposición a estos riesgos.
>
> Para lograr este objetivo, el Ministerio de Trabajo y Seguridad Social implementa un Sistema de Gestión de Seguridad de la Información (SGSI), basado en la Norma INTE/ISO/IEC 27000:2018 y su familia normativa, en las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información N-2-2007-CO-DFOE de la Contraloría General de la República, así como las mejores prácticas internacionales, con el fin de proteger los activos de información Institucional. (p. 8)

Fases Para Implementación de un SGSI

En la fase inicial, se debe definir la política, seguidamente definir el alcance del SGSI para limitar el mismo, en la fase tercera se debe realizar un análisis de riesgos, en la que se analizan los activos de información y se definen las amenazas y vulnerabilidades. Seguidamente, la gestión del riesgo, desde el punto de vista organizacional y se debe determinar el grado de aseguramiento requerido, en la siguiente fase se realiza la selección de controles a implementar, que son los controles propuestos por la Norma, más los controles que se consideren adicionales, seguidamente se realiza la declaración de aplicabilidad, de la misma manera serán los propuestos por la normal y finalmente una revisión del sistema, que incluye medidas preventivas, correctivas y propuestas de mejora, de esta forma se garantiza un plan de auditorías.

Los riesgos de la seguridad de la información representan una amenaza considerable para las empresas, esto se debe a una posible pérdida financiera o daño, pérdida de servicios esenciales para la continuidad de negocio y la reputación y confianza de los clientes. Es por esto que la gestión de riesgos es uno de los elementos clave cuando se trata de prevención de algún tipo de fraude en línea, robo de identidad, pérdida de datos personales entre otros incidentes, sin un marco de gestión

de riesgos sólido y claro, definido y bien conocido para la empresa, la organización se expone a todos estos tipos de amenazas y delitos informáticos. El diseño y la implementación de un SGSI, otorgará confianza a las clientes y proveedores de que la seguridad de su información es tomada con seriedad y prioridad, estando a la vanguardia en la aplicación de técnicas y procesos para hacer frente a dichas amenazas y problemas de la seguridad.

El concepto de riesgo cibernético emerge como una sombra constante en este escenario digital. En este contexto, la empresa necesita abordar la identificación, evaluación y gestión de estos riesgos de manera proactiva. La norma ISO/IEC 27005, especializada en la gestión de riesgos de seguridad de la información, se convierte en una guía valiosa para desarrollar un enfoque sistemático y efectivo. Al comprender y mitigar los riesgos, CORGIA asegura no solo su seguridad actual, sino también su resiliencia ante las amenazas futuras.

La noción de auditoría de seguridad se eleva como una herramienta esencial para evaluar la efectividad de las medidas implementadas. La aplicación de estándares como ISO/IEC 27001 establece un marco que no solo exige controles y políticas de seguridad, sino también la realización de auditorías periódicas. La auditoría, entonces, se convierte en un instrumento crítico para validar la conformidad con los estándares y garantizar que los controles de seguridad estén operando de manera eficiente.

Acompañando este recorrido, se integran normas adicionales COBIT, NIST SP 800-46 e ITIL. Estas directrices aportan una estructura adicional y establecen mejores prácticas para la gestión de la seguridad y la gobernanza de las tecnologías de la información. ISO/IEC 27002, centrada en la gestión de la seguridad de la información, y COBIT, especializada en el gobierno de las tecnologías de la información, delinean roles y permisos, creando un marco sólido que resguarda la integridad y confidencialidad de la información (UNE-EN ISO/IEC 27002, 2017) (ISACA Costa Rica Chapter, 2019)

NIST SP 800-46 e ITIL

NIST SP 800-46 se posiciona como una brújula que orienta hacia el terreno del teletrabajo, proporcionando pautas claras para fortalecer aspectos clave como la autenticación, encriptación y monitoreo de actividades (NIST, 2016). Mientras tanto, ITIL, reconocida por sus prácticas para la

gestión de servicios de tecnologías de la información, prepara el terreno para una implementación segura y eficiente, asegurando la alineación de los servicios con los objetivos empresariales (Axelos, 2024).

En el proceso de optimización respaldado por estándares internacionales, la tecnología moderna se convierte en un elemento clave. La integración de firewalls, sistemas de detección y prevención de intrusiones, junto con la implementación de redes virtuales privadas (VPN), conforma una infraestructura que se fortalece ante las amenazas cibernéticas.

Este panorama se enriquece mediante la adopción de políticas y protocolos de seguridad basados en estándares reconocidos. La coherencia en la configuración de la seguridad de dispositivos adquiere un papel fundamental, abordando aspectos como la instalación de antivirus, cortafuegos y otras medidas esenciales. Este enfoque, respaldado por normativas como NIST SP 800-53 e ISO/IEC 27001, que tiene como objetivo establecer estas pautas para una defensa coherente y robusta contra las amenazas cibernéticas.

La estrategia de gestión de copias de seguridad, en consonancia con la normativa ITIL, se implementa con meticulosidad para garantizar la continuidad del negocio. Este enfoque se traduce en la automatización precisa del respaldo, asegurando la periodicidad y consistencia necesarias. La segmentación eficiente de datos se convierte en un componente crítico, permitiendo una organización lógica y eficaz de la información, mientras que los procedimientos de prueba meticulosos se aplican para validar la integridad y la capacidad de recuperación del sistema.

Un elemento clave dentro de esta estrategia es el plan de capacitación del personal, diseñado para dotar a los colaboradores con las habilidades y conocimientos necesarios para interactuar eficientemente con el sistema de copias de seguridad. La concientización se integra de manera complementaria, destacando la importancia de la participación y responsable de cada miembro en el cuidado de la información crítica de la organización.

Este enfoque holístico no solo tiene como objetivo la mera adopción de estándares y tecnologías modernas, sino la integración profunda de prácticas sólidas en la rutina operativa de Corgia Gestión e Ingeniería Alternativa. La visión es construir un futuro donde la empresa no solo

alcance la optimización operativa, sino que también establezca un paradigma de seguridad perdurable en la compleja era digital actual.

Seguridad de la Información

Métodos de Seguridad Informática

Anteriormente, se mencionó la importancia de contar con herramientas modernas en la actual era digital como lo son productos de ciberseguridad, en el mercado y el marco de la informática, el firewall, o cortafuegos, emerge como un componente esencial en la protección de sistemas y redes. Este software o hardware (se puede optar por cualquiera de las dos opciones, que realizan las mismas funciones) se configura para filtrar el tráfico de datos y prevenir accesos no autorizados, estableciendo un perímetro defensivo para salvaguardar la integridad y confidencialidad de la información (Chapple, 2019, párr. 1). De la misma manera, se sugiere contar con un "Sistema de Detección de Intrusos (IDS, por sus siglas en inglés) que constituye otra capa de defensa. Este sistema monitorea activamente la red en busca de patrones o comportamientos anómalos que puedan indicar intentos de acceso no autorizado o actividades maliciosas. Su función es alertar a los administradores ante posibles amenazas para que puedan tomar medidas preventivas." (Roesch, 1999, pp. 229-238)

Las herramientas de monitoreo y auditoría son vitales para evaluar y registrar las actividades en la red. Estas soluciones proporcionan una visión detallada del tráfico, el rendimiento del sistema y el comportamiento de los usuarios. "A través de registros y análisis, los administradores pueden identificar posibles vulnerabilidades o comportamientos sospechosos." (Vallis, 2017).

En la esfera de la seguridad informática, las soluciones VPN (Redes Privadas Virtuales) son fundamentales para garantizar la seguridad en las comunicaciones. Estas redes cifran el tráfico de datos, permitiendo a los usuarios acceder de forma segura a recursos de la red desde ubicaciones remotas. Además, establecen un canal seguro para la transmisión de información sensible (Rouse, 2018). Estos componentes, al integrarse estratégicamente, conforman un robusto entramado de

seguridad que fortalece la postura de CORGIA Gestión e Ingeniería Alternativa ante las amenazas cibernéticas.

El concepto de ciberseguridad, que abarca medidas más amplias para proteger los sistemas, redes y programas, se entrelaza con la propuesta de seguridad de la información de CORGIA. La adopción de prácticas y tecnologías modernas, como la ciberseguridad basada en inteligencia artificial y el análisis de comportamiento, se convierte en una necesidad. CORGIA no solo responde a las amenazas actuales, sino que también se anticipa a los desafíos emergentes en la era digital en la que nos encontramos.

Recopilación, Manejo y Gestión de Datos

Estos anteriores con la finalidad de poder asegurar una continuidad operativa o, en otras palabras, continuidad de negocio que (Internation Standard ISO 22301, 2019) define esto como los procesos y capacidad de la organización para continuar suministrando productos o servicios a niveles predefinidos aceptables, posterior a un incidente disruptivo. Por lo que también es necesario contar con un proceso de recuperación de datos efectivo, que según (IBM, s.f.):

> La recuperación de datos empresariales es el proceso de restaurar datos perdidos, dañados, eliminados accidentalmente o de otro modo inaccesibles en su servidor, sistema, dispositivo móvil o dispositivo de almacenamiento (o en un nuevo dispositivo si el dispositivo original ya no funciona). (párr. 2)

De la mano de la recuperación de datos y la continuidad de negocio, que se encuentra relacionada a los datos que la empresa considera necesarios para realizar todos sus procesos internos, viene un concepto que se conoce como la tríada CIA, que la Universidad Pontificia nos explica en el artículo a continuación (Comillas Universidad Pontificia, 2023):

> La tríada CIA del inglés o CID de Confidencialidad, Integridad y Disponibilidad se considera la base de la seguridad de la información. Cada control de seguridad y cada vulnerabilidad de seguridad pueden considerarse a la luz de uno o más de estos conceptos clave. Para que un programa de seguridad se considere exhaustivo y completo, debe abordar adecuadamente toda la tríada CID.

> Confidencialidad significa que los datos, objetos y recursos están protegidos contra la visualización y otros accesos no autorizados.
>
> Integridad significa que los datos están protegidos de cambios no autorizados para garantizar que son fiables y correctos.
>
> Disponibilidad significa que los usuarios autorizados tienen acceso a los sistemas y recursos que necesitan. (p. 1-4)

Sin embargo, no es posible tener un sistema de recuperación de datos efectivo si realmente no se conoce en qué consiste el mismo y qué componentes lo componen, por lo que (IONOS, 2022) nos define una copia de seguridad como una disposición para mantener el funcionamiento en caso de emergencia, en sistemas digitales, las copias de seguridad o bien *backups* en inglés, son datos almacenados de forma redundante, y se distribuyen en diferentes soportes. Los backups son especialmente importantes en dos circunstancias, que IONOS enumera como la pérdida de datos, en este escenario permitiría reconstruirse a partir de una copia de seguridad y cambio de datos, que pueden ser restablecidos a partir de un estado anterior.

Para definir una estrategia de *backups* o respaldos, la cuál es necesaria ya que estos son valiosos sólo si se planifican y se crean con previsión, es necesario que incluya ciertas consideraciones básicas, así como qué datos hay que hacer una copia de seguridad, no toda la información es crucial para la continuidad de negocio y en caso de hacer nuestro sistema de copias de seguridad en la nube, puede llegar a ser costoso mantener constantes copias de toda la información, incluso la que no es requerida. Definir con qué frecuencia se realizarán estas copias de seguridad, en qué se estarán realizando, ya sea un dispositivo físico (en el que se deberá planificar su constante crecimiento y capacidad) o en la nube, en la que se deben tener consideraciones de planes, licencias entre otros. Con qué métodos se realizarán dichas copias, de forma manual o automatizada, entre otros. Y finalmente, saber cómo garantizar la integridad de estas copias y cómo se restauran en caso de ser necesario. Estos últimos suelen descuidarse y para el momento de una emergencia, se entorpece el proceso.

La empresa actualmente cuenta con un tipo de almacenamiento, híbrido y se ha mencionado que mantienen sus copias de seguridad en dispositivos de almacenamiento, por lo que

se define a continuación los tipos existentes para una mejor comprensión de lo que se utiliza, según (IBM, s.f.):

> El almacenamiento de conexión directa o DAS, funciona como su propio nombre indica. Este almacenamiento suele estar en una zona cercana y directamente conectado a la máquina que accede a él, que a menudo es la única máquina conectada. DAS también proporciona servicios de copia de seguridad locales, pero el uso compartido es limitado. Los dispositivos DAS incluyen disquetes, discos ópticos como los discos compactos (CD) y los discos de video digital (DVD), unidades de disco duro (HDD), unidades flash y unidades de estado sólido (SSD).
>
> El almacenamiento en red permite que más de un ordenador acceda a él a través de una red, lo que es mejor para compartir datos y colaborar. Su capacidad de almacenamiento externo también lo hace más adecuado para copias de seguridad y protección de datos. Dos configuraciones comunes de almacenamiento basadas en red son el almacenamiento conectado a la red (NAS) y la red de área de almacenamiento (SAN). (párr. 8-9)

Se ha respaldado a lo largo de este documento que la segunda opción es altamente recomendada para ser utilizada en esta nueva transformación y migración digital a la que se expone la empresa CORGIA, con todas las ventajas y facilidades que ofrece la misma, sin embargo, es positivo reconocer la importancia de ambas opciones.

Transformación Digital

En la constante práctica de mejorar la infraestructura actual de la empresa CORGIA Gestión e Ingeniería, ha surgido el término de la transformación digital, ya que esta empresa cuenta con muchos procesos que se realizan de forma manual y cuentan con inventario y dispositivos únicamente locales, por lo que (AWS, 2023) nos define este concepto de la siguiente manera:

> La transformación digital es el proceso mediante el cual una organización integra tecnología digital a todas las áreas empresariales. Este proceso cambia por completo la forma en que una organización ofrece valor a los clientes. Las empresas adoptan

> tecnologías digitales innovadoras para realizar cambios culturales y operativos que se adapten mejor a las necesidades cambiantes de los clientes. (párr. 1)

Y se comenta que es importante porque aporta beneficios que esta transformación brinda, ya que mejora la productividad, las tecnologías emergentes como lo son servicios en la nube, por ejemplo, nos ahorran tiempo y mejorar la eficiencia en los procesos empresariales. También otro beneficio es que mejora la experiencia del cliente, en la era postpandemia, se espera una disponibilidad de servicio constante y a través de múltiples canales, sin embargo, esto mismo aporta a la creciente demanda por lo que los sitios web y sistemas de comunicación se espera que sean fáciles y cómodos de utilizar bajo cualquier entorno. Finalmente, otro beneficio que se puede mencionar y muy importante, es la reducción de los costos operativos, la inversión inicial puede ser costosa, sin embargo, puede reducir significativamente los costos operativos actuales, pueden optimizarse procesos empresariales existentes y reducir costos de mantenimiento de equipo, logística, recursos humanos entre otros.

Retorno de Inversión

Una vez comprendidos los beneficios que conlleva la transformación digital, se debe comprender qué es el retorno de inversión (ROI), que es importante obtenerlo para considerar si es beneficioso para la empresa invertir en dicho proyecto, según (Westreicher, Retorno de la inversión (ROI), 2020), “El retorno de la inversión (ROI) es un indicador que nos permite evaluar la rentabilidad de una inversión en base al capital destinado y al beneficio obtenido.” (párr. 1)

Este retorno de inversión debe de ser evaluado personalmente por los directivos de la empresa, anteriormente se ha mencionado los *stakeholders* del proyecto, en otras palabras, estos podrían ser los encargados de aprobar la viabilidad del proyecto según las proyecciones que se puedan comprobar a lo largo de la investigación, según (ASANA, 2023):

> Los *stakeholders* del proyecto son las partes interesadas que pueden influir o verse afectadas por el proyecto en el que estás trabajando. Los participantes pueden provenir de todos los niveles de la organización, desde colaboradores individuales hasta ejecutivos sénior, pero si están involucrados en tu proyecto, son importantes. Incluso si los

participantes no están directamente involucrados en el trabajo del día a día del proyecto, de todas formas, pueden verse afectados por su resultado.

De la mano de la transformación digital que se ha mencionado y como parte de la inversión principal de este proyecto, se basa en la modernización de la infraestructura de red que gracias a (Tecnología Mix, 2023) entendemos la infraestructura de red como todos los recursos de una red que hacen posible la conectividad, la gestión, las operaciones comerciales y la comunicación de la red o Internet. La infraestructura de red comprende hardware y software, sistemas, dispositivos, y permite la informática y la comunicación entre usuarios, servicios, aplicaciones y procesos. Todo lo que esté involucrado en la red, desde servidores hasta enrutadores inalámbricos, se une para formar la infraestructura de red de un sistema. La infraestructura de red permite una comunicación y un servicio efectivos entre usuarios, aplicaciones, servicios, dispositivos, etc.

Consideraciones de una empresa en vías de digitalización

Al tener una infraestructura de red en vías de digitalización, es crucial mantenerse actualizado en temas de la seguridad de red, nuevas amenazas cibernéticas que puedan surgir y principalmente cómo protegerse de las mismas para prevenir cualquier tipo de desastre. De acuerdo con (Cisco, 2024) “La seguridad de red es cualquier actividad diseñada para proteger el acceso, el uso y la integridad de la red y los datos corporativos.” (párr. 1), en la que se definen los siguientes tipos de seguridad:

> Los firewalls ponen una barrera entre su red interna de confianza y las redes externas que no son de confianza, como Internet. Usan un conjunto de reglas definidas para permitir o bloquear el tráfico. Un firewall puede ser hardware, software o ambos. Cisco ofrece dispositivos de gestión unificada de amenazas (UTM) y firewalls de próxima generación centrados en las amenazas.
>
> Seguridad del correo electrónico, los gateways del correo electrónico son el principal vector de amenaza para las infracciones a la seguridad. Los atacantes usan la información personal y las tácticas de ingeniería social para desarrollar campañas de suplantación de identidad (phishing) sofisticadas para los destinatarios de los dispositivos a fin de dirigirlos a sitios con malware. Una aplicación de seguridad de correo electrónico bloquea los

> ataques entrantes y controla los mensajes salientes para prevenir la pérdida de datos sensibles.
>
> Software antivirus y antimalware, el "malware", abreviatura de "software malicioso", abarca los virus, gusanos, troyanos, ransomware y spyware. En algunos casos, el malware puede infectar una red y permanecer latente por días o incluso semanas. Los mejores programas antimalware no solo detectan la entrada de malware, sino que también hacen un seguimiento constante de los archivos para detectar anomalías, eliminar malware y reparar daños. (párr. 4-6)

Por otra parte, es importante tener presente que como parte de las soluciones que se propondrán para este proyecto de investigación que son requeridas, está la segmentación de la red, ya que la segmentación definida por software clasifica el tráfico de red en distintas categorías y facilita la aplicación de políticas de seguridad. Lo ideal es que las clasificaciones se basen en la identidad de los EndPoints no solo en las direcciones IP. Ya que de esta manera que puede asignar derechos de acceso basados en roles, ubicación y demás, de modo que se otorgue el nivel de acceso correcto a las personas adecuadas, lo que nos conduce al control de accesos, no todos los usuarios deben tener acceso a la red. Para evitar posibles ataques, debe reconocer a todos los usuarios y dispositivos. Entonces se podrá aplicar las políticas de seguridad, se puede bloquear dispositivos de *EndPoint* que no cumplen las políticas o proporcionarles acceso limitado. Este proceso se denomina control de acceso a la red (NAC) según (Cisco, 2024).

Al contar con un sistema digitalizado en su mayoría, puede tornarse complejo aprender a tener control sobe su estado y lo que sucede dentro de nuestro sistema, por lo que de acuerdo con (KPMG, 2020):

> Al rediseñar los enfoques tradicionales de auditoría, para que sean repetibles y sostenibles en el tiempo, nos encontramos con los conceptos de auditoría continua y monitoreo continuo, permitiendo identificar en forma temprana, deficiencias de control y ayudando a mitigar rápidamente los problemas que puedan surgir en el futuro.

> Le permiten realizar un seguimiento de los controles, transacciones y eventos de negocios, en la medida que van ocurriendo, ayudando así a garantizar el cumplimiento de las políticas, procedimientos y regulaciones.
>
> Estos conceptos, utilizados correctamente, pueden ayudarle a gestionar de mejor manera su exposición a los riesgos claves.
>
> Los avances tecnológicos actuales, hacen que las herramientas necesarias para su implementación sean de más fácil acceso y de un menor costo, permitiendo así, vigilar con una inversión razonable, los riesgos y fallas de control que pueden comprometer la integridad de la organización. (párr. 1-5)

Se puede concluir que la implementación de enfoques de auditoría y monitoreo continuo son cruciales para adaptarse al entorno digitalizado al que se desea llegar. El uso en conjunto de todos estos controles no solo permite identificar las deficiencias de controles de manera temprana si no que contribuye a mitigar rápidamente los problemas a los que se puedan enfrentar en un futuro. Al seguir de cerca los controles, transacciones y eventos en tiempo real que ocurren en la empresa, se garantiza el cumplimiento de las políticas, procedimientos y regulaciones que se establecen a lo largo de esta investigación.

Leyes y Regulaciones en Costa Rica

Cuando se aborda el tema de leyes y regulaciones en Costa Rica en relación con el uso de software y el tratamiento de datos personales, es importante considerar diversos aspectos que impactan tanto a las empresas como a los individuos. Estas regulaciones no solo tienen el propósito de garantizar el cumplimiento legal, sino también de proteger los derechos fundamentales de las personas y promover un entorno digital seguro y confiable.

Para todas estas soluciones que se proponen, como se ha desglosado en el apartado de la viabilidad económica, se deben pagar ciertas licencias de software para poder hacer uso de soluciones digitales que ofrecen las compañías, pero ¿qué es esto y para qué sirven?, según (SOLBYTE, 2022):

> Hay que tener muy en cuenta que el software ilegal puede causar grandes perjuicios a una empresa, tanto en términos financieros como de credibilidad ante sus clientes.
>
> Cuando la empresa propietaria de los derechos del software es informada sobre ello, emitirá un aviso de auditoría contra la empresa infractora. De cara a esta, la organización empresarial que haya cometido la infracción deberá asegurarse de que tiene los registros de compra correspondientes. Ignorar el aviso de auditoría puede dar lugar a una demanda judicial de la empresa propietaria.
>
> Cuando se emplea un determinado software, este sigue perteneciendo a la empresa proveedora. Los términos de la licencia están determinados por el proveedor, y en realidad el que adquiere el software no se convierte en propietario sino en licenciatario del mismo. Se paga, pues, por el uso del software, y no por su propiedad. (párr. 1-3)

La necesidad de adquirir licencias de software legales se destaca como un requisito fundamental para evitar posibles repercusiones financieras y legales. El uso de software ilegal puede acarrear consecuencias graves, incluyendo demandas judiciales por parte de las empresas propietarias de los derechos del software. Además, es importante comprender que, al adquirir software, en realidad se está obteniendo una licencia de uso y no la propiedad de este, lo que implica que se deben respetar los términos y condiciones establecidos por el proveedor.

Ley de Protección de la Persona Frente a Tratamiento de sus Datos Personales

Ahora, surge la incógnita de si existen regulaciones para respaldar y definir el correcto tratamiento de datos personales, que las empresas generalmente manejan de forma masiva, o como clientes de las mismas, cómo podremos suscribirnos, comprar sus licencias o bien como sus funcionarios otorgar acceso a cierta información personal, de la misma manera si existe algún tipo de consecuencias ante su incumplimiento, para esto (Tribunal Supremo de Elecciones, 2011) nos proporciona el objetivo y fin de la Ley de Protección de la Persona Frente a Tratamiento de sus Datos Personales Ley n.º 8968:

> Esta ley es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos

> fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes. (p. 1)

Por otro lado, las leyes relacionadas con la protección de datos personales buscan salvaguardar la autodeterminación informativa de las personas y garantizar sus derechos fundamentales en relación con la privacidad y la seguridad de sus datos. La Ley de Protección de la Persona Frente a Tratamiento de sus Datos Personales establece claramente el objetivo de garantizar estos derechos, independientemente de la nacionalidad o residencia de las personas.

Ley Para Reprimir y Sancionar los Delitos Informáticos en Costa Rica

Así como la Ley N.º 4573 Para Reprimir y Sancionar los Delitos Informáticos en Costa Rica que según el (Sistema Costarricense de Información Jurídica, 2024):

> El que, por medio del uso indebido de las Tecnologías de la Información y la Comunicación, valiéndose de cualquier manipulación en sistemas informáticos o cualquiera de sus componentes, datos informáticos o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho para sí o para un tercero en perjuicio ajeno, será sancionado (párr. 2)

Asimismo, la legislación para reprimir y sancionar los delitos informáticos juega un papel crucial en la protección de la seguridad digital. Esta ley busca combatir el uso indebido de las tecnologías de la información y la comunicación, así como cualquier manipulación en sistemas informáticos que pueda causar perjuicio a terceros. La imposición de sanciones por parte de esta ley busca disuadir la comisión de delitos informáticos y promover un uso ético y responsable de la tecnología.

En conclusión, el cumplimiento de las leyes y regulaciones en materia de software, protección de datos y delitos informáticos es esencial para garantizar la seguridad y el bienestar tanto de las empresas como de los individuos en un entorno digitalizado. Estas regulaciones no solo proporcionan un marco legal para el uso de la tecnología, sino que también contribuyen a fomentar la confianza y la transparencia en las interacciones digitales.

Cada concepto de los que se han mencionado a lo largo de este marco referencial no solo representa una capa adicional de seguridad, sino también una pieza clave en la construcción de un entorno empresarial digital eficiente y sostenible. En esta travesía hacia la optimización y seguridad, CORGIA no solo responde a los desafíos actuales, sino que también se prepara para liderar en el panorama digital en evolución.

CAPÍTULO III: MARCO METODOLÓGICO

El marco metodológico es un componente fundamental en una investigación, ya que nos proporciona la estructura y el enfoque en el que se guiará el proceso investigativo, en este, se definen el conjunto de métodos, técnicas y procedimientos para recolectar y analizar los datos, así también como la forma en la que se interpretarán los resultados obtenidos.

De la misma manera, se define cómo se llevará a cabo el estudio que se realizará para identificar los problemas de la empresa CORGIA, qué tipo de datos se recopilarán, cómo se analizará y procesará esta información y qué criterios se utilizarán para interpretar los hallazgos. Es decir, proporciona un plan detallado que orienta el proceso de investigación, asegurando que se sigan prácticas rigurosas para obtener conclusiones confiables y respuestas robustas, que se puedan respaldar.

Enfoques de Investigación

El enfoque es "una manera de ver las cosas o las ideas y, en consecuencia, también de tratar los problemas relativos a ellas." (Bungee & Ardilla, 2002). Enfoque se refiere sobre todo a la naturaleza del estudio que se realiza, y este se abarca en todas sus etapas, desde la definición del tema, el planteamiento del problema que se investigará, hasta el desarrollo de la perspectiva teórica, la definición de la estrategia metodológica y la forma de recolección, análisis e interpretación de los datos.

El propósito fundamental de una investigación es generar conocimiento nuevo que sirva para la solución de algún problema, ya sea teórico, práctico o una mezcla de ambos. El enfoque de la investigación es un proceso sistemático y controlado que está directamente relacionado con los métodos de investigación. A través de la historia, surgen varias corrientes de pensamiento, pero estas se concentraron en dos enfoques principales de la investigación, el cualitativo y cuantitativo. De estas, se deriva el enfoque mixto, que consiste en una combinación de ambas, como su nombre lo indica.

Cada enfoque lleva consigo una manera particular de concebir y abordar el objeto de estudio, lo cual influye en la definición del problema, la elección de la teoría que fundamenta la investigación y la metodología empleada para recolectar, analizar e interpretar los datos. Además,

la elección de un enfoque específico también está determinada por la naturaleza del problema que se pretende abordar y por los recursos disponibles para llevar a cabo la investigación.

Enfoque Cualitativo

El enfoque cualitativo se orienta más hacia la descripción profunda de un fenómeno con la finalidad de comprenderlo y explicarlo a través de la aplicación de métodos y técnicas derivadas de sus concepciones y fundamentos. Según el libro Diseño de la Investigación Métodos Cualitativo, Cuantitativo y Mixto, se han generado varias descripciones y definiciones de formas en las que se conduce un estudio cualitativo, que se comparten a continuación:

Según John W, 2009 quién toma referencia de Creswell 2007, la etnografía se define como una estrategia donde el investigador estudia todo un grupo cultural en un escenario natural durante un tiempo prolongado, con la finalidad de colectar principalmente datos observacionales y de entrevistas, este proceso es flexible y típicamente evoluciona en respuesta a las realidades vividas que se encuentran en su escenario natural.

La teoría sustentada según Charmaz 2006, Stauss 1990 y Corbin 1998 a través de John W, es una estrategia de indagación en la que el investigador deriva de una teoría general, varias teorías abstractas de un proceso, acción o interacción que se sustenta en puntos de vista de los participantes. El mismo proceso involucra múltiples etapas de recolección de datos y refinamiento e interrelación de distintas categorías de información. Dos características que figuran como principales en este diseño de investigación, son las constantes comparaciones de los datos con categorías emergentes de diferentes grupos para maximizar las similitudes y diferencias entre la información.

Según Stake 1995, a través de John W, existe también la definición para los llamados estudios de caso que son una estrategia en la que le investigador explora a profundidad un programa, un evento, una actividad, un proceso o uno o más individuos, estos casos son limitados por tiempo o actividad y dichos investigadores recolectan la información haciendo uso de varios procedimientos de recolección de datos en un periodo sostenido de tiempo.

La investigación fenomenológica es otra estrategia que se define a través de John W para este enfoque cualitativo, referenciando Nieswiadomy 1993, en la que el investigador identifica la

esencia de las experiencias que se han tenido acera de un fenómeno que es descrito por los participantes. Se debe comprender a cabalidad las experiencias vividas, por lo que involucra estudiar un número pequeño de temas en los cuales el compromiso extensivo y prolongado es para desarrollar patrones y relaciones de significado, a lo largo de este proceso el investigador pone de lado sus experiencias propias vividas con la finalidad de entender las de los participantes en estudio.

Por último, dentro de las definiciones que nos aporta John W dentro del enfoque cualitativo quién referencia a Clandinin y Connelyy 2000, la investigación Narrativa que es una estrategia de indagación en la que el investigador, estudia la vida de los individuos y pregunta a uno o más para que compartan historias acerca de sus vidas, a menudo la información es reescrita por el investigador en una narrativa cronológica, finalmente la misma combina los puntos de vista de vida de los participantes en una misma narrativa colaborativa.

Finalmente, se puede basar una investigación cualitativa en alguno de estos caminos conductores que han sido definidos por los autores mencionados o una combinación de las anteriores para complementar una buena investigación de este tipo, siempre y cuando se acople a las necesidades esta.

Enfoque de Investigación Seleccionado

Para llevar a cabo esta investigación, se ha seleccionado un enfoque cualitativo, esto porque es el enfoque que más se acerca la realidad de esta investigación, el tipo de datos que se debe recolectar para conducir esta y la forma en la que se debe manejar y procesar los mismos para obtener un resultado satisfactorio.

En detalle, se enfoca en la comprensión profunda de las necesidades, desafíos y soluciones en temas de seguridad de la información y tecnología, que experimenta la empresa CORGIA. De la misma manera se presenta una descripción detallada de tecnologías específicas recomendadas para mejorar la infraestructura, que es uno de sus problemas principales. Se basa en referentes internacionales y se rige bajo Leyes específicas que son mencionadas a lo largo de la investigación.

De acuerdo con la teoría anteriormente mencionada, el enfoque de esta investigación se acerca a la teoría sustentada ya que la misma aclara que en este diseño se centra en las

comparaciones constantes de datos con categorías emergentes y ejemplificación teórica de diferentes grupos para maximizar las similitudes y diferencias de información, tal como lo hacemos con la infraestructura actual que posee la empresa y las tecnologías emergentes que se sugieren para lograr su transformación digital y migrar hacia una infraestructura moderna.

Método de la Investigación

Según el libro de fundamentos de Investigación, “El alcance es una especie de "pivote" entre lo que encontraste en la revisión de la literatura y la formulación de la hipótesis. Del alcance dependerá tu estrategia de investigación, incluido el diseño, los procedimientos y otros elementos.” (Sampieri, Valencia, Torres, & Romo, 2017)(p. 74). Contamos con cuatro alcances que son: exploratorio, descriptivo, correlacional y explicativo.

Cualquier investigación puede ser dirigida en uno de estos alcances o varios de estos, es decir, combinar estos tipos de investigación a través de su desarrollo, ya que algunos estudios de un tipo, suelen ser la base de otro, de la misma manera, puede tener un alcance distinto a lo largo de cada una de las etapas de la investigación.

Investigación Descriptiva

Con este tipo de estudio, se busca recolectar datos sobre diversos conceptos o componentes del fenómeno que se investiga, según (Sampieri, Valencia, Torres, & Romo, 2017):

> Con los estudios descriptivos se busca especificar las propiedades, características y perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Es decir, miden o recolectan datos sobre diversos conceptos (variables), aspectos, dimensiones o componentes del fenómeno que se investiga. En un estudio descriptivo, el investigador selecciona una serie de cuestiones (que denominamos variables) y después recaba información sobre cada una para representar 10 que se investiga (describirlo). (p. 76) (párr. 3)

Por lo que podemos entender que su finalidad es especificar las propiedades, características y perfiles de procesos, objetos o cualquier otro fenómeno que se someta a un análisis.

Tipo de Investigación Seleccionado.

El enfoque de investigación elegido como descriptivo se justifica por la naturaleza detallada y minuciosa del análisis presentado en esta investigación. Se centra en describir exhaustivamente una situación, fenómeno o problema particular, brindando una visión clara y completa de los elementos involucrados. Específicamente este caso de estudio es sobre la infraestructura tecnológica y la seguridad informática de CORGIA Gestión e Ingeniería Alternativa, a lo largo de la investigación se presenta una descripción detallada de la situación actual de la empresa, incluyendo su infraestructura de hardware, sus necesidades específicas y los desafíos que enfrenta en términos de seguridad y acceso remoto.

Además, el enfoque descriptivo se adapta adecuadamente a la propuesta de mejoras y soluciones que se presentan para solucionar los problemas identificados. Al describir de manera detallada las tecnologías y prácticas recomendadas para optimizar la infraestructura tecnológica y fortalecer la seguridad informática de la empresa, se proporciona una guía clara y completa para la implementación de estos cambios. Esto incluye la integración de normativas y estándares internacionales reconocidos, como ISO/IEC 27001, COBIT, NIST SP 800-46 y Mejores Prácticas de ITIL, lo que contribuye a una descripción precisa y detallada de las recomendaciones propuestas.

En resumen, el enfoque descriptivo se justifica por la necesidad de proporcionar una descripción detallada y completa de la situación actual de la empresa, así como de las recomendaciones para mejorar su infraestructura tecnológica y seguridad informática. Esto permite una comprensión profunda de los problemas y desafíos enfrentados por la empresa, así como una guía clara para la implementación de soluciones efectivas.

Fuentes de Información

Las fuentes de información son todos aquellos recursos que son utilizados para obtener datos sobre algún tema. Cuando una investigación es llevada a cabo, es necesario contar con múltiples fuentes de información que, cualquier usuario pueda consultar y confirmar su existencia, de estas se recaba información de un tema de interés y se profundiza o se termina de detallar con la opinión. Es importante tener presente que, de acuerdo al tipo de investigación, que los hemos

detallado anteriormente, y su objetivo de estudio, se debe investigar de ante mano ya que existen múltiples formatos y fuentes de investigación, los mismos van desde libros, periódicos, encuestas, documentos de instituciones públicas reconocidas, videos, entrevistas entre otros.

Cada fuente se puede considerar o bien, evaluar como confiable, de acuerdo con la veracidad de la información y qué tanto sea comprobable. Por esto, es recomendado comparar los datos entre distintas fuentes de información y saber el recorrido o reconocimiento de la fuente.

Fuentes de Información Primaria

Las fuentes de información primaria son consideradas todas aquellas que contienen la información original, algunas de sus categorías según (LiFeder, 2024):

> Revistas: publicaciones periódicas que pueden ser tanto especializadas como enfocadas a la divulgación entre el público en general. Se puede acceder a ellas por medios electrónicos o en su formato tradicional impreso. Libros: obras impresas o electrónicas que hablan sobre la época o tópico que se está investigando. Monografías: documentos explicativos que desglosan un tema en particular; usualmente cuentan con recursos visuales de apoyo. Se caracterizan por su lenguaje sencillo y son de extensión variable. Es posible encontrarlas impresas o digitales. Periódicos: fuente de publicación diaria que brinda información de contexto sobre un hecho o momento en particular.
>
> Cartas: documentos epistolares que dan cuenta de crónicas, pensamientos y vida personal de quienes los escribieron. Resultan interesantes para acercarse a la mirada particular de alguien que vivió en determinada época y presenció ciertos hechos. Discursos: textos elaborados para participar en una exposición o presentación pública. Leyes: normas de rango legal que fueron dictadas por las autoridades; establecen mandatos y prohibiciones. Manuscritos: textos que no fueron publicados y que dan cuenta de la postura de quien los escribió sobre un suceso o hecho determinado. Entrevistas: diálogo establecido con testigos o personas involucradas en un hecho o situación particular. Videos/películas: documentales, series y material audiovisual que contiene información original sobre un tema. (párr. 5-14)

Fuentes de Información Secundaria

Las fuentes de información secundaria son aquellas que no contienen la información en su totalidad, si no que hacen referencia a fuentes primarias, en las que se indica que se podría encontrar más información sobre este tema. Algunas de estas fuentes son las enciclopedias, estas suelen resolver dudas sencillas, o ser definiciones de conceptos, brindan información con la intención de ampliar el conocimiento en un tema específico. Así como los diccionarios, que son referencias que colectan términos y vocabulario para definir o aclarar un significado.

Por otra parte, encontramos las estadísticas, que es un instrumento que se utiliza para presentar datos o bien gráficos que resumen visualmente información relevante, esto permite analizar patrones lo que facilita la obtención de datos clave para futuras tomas de decisiones o bien analizar su comportamiento. Las bases de datos permiten manejar grandes volúmenes de información, datos y contenido, normalmente son colecciones que se enfocan o relacionan entre sí. Finalmente, otro tipo de información secundaria a destacar son las antologías, estas son una colección de textos de un mismo autor o tema.

Fuentes de Información Terciaria

Estas fuentes de información terciarias son las que explican un tema o lo resumen sin citar fuentes de referencia, o bien hacen referencia a otras fuentes como las primarias o secundarias. Estas fuentes se pueden encontrar en internet, bibliografías que son listados de libros u otras fuentes de consulta, alojadas en blogs, catálogos que describen brevemente otros libros, documentos u obras, páginas electrónicas, artículos de encuentras que son notas que recopilan y presentan la información publicada en encuestas, entre muchas otras.

Sirven en algunos casos para orientarse sobre temas, pero tienen menos autoridad que las anteriores. Por lo general, no se citan en un trabajo académico si no se tiene la certeza de que la información que presentan haya sido corroborada y respaldada por expertos, por lo tanto, carece de veracidad.

Variables o Unidades de Análisis

Las variables de investigación se caracterizan porque son inestables, es decir, puede cambiarse o modificarse en cualquier momento, estos factores pueden ser medidos o bien manipulados, es todo aquello que puede estudiarse y ser controlado a través de una investigación. Su particularidad se basa en que sufre cambios que se pueden observar, medir y ser objeto de análisis durante el proceso de una investigación.

Una variable es una propiedad del objeto en estudio que puede asumir dos o más valores, en otras palabras, que puede cambiar. Si esto no ocurre, la característica observada y en estudio es realmente una constante. Específicamente en una investigación, las variables se trabajan de acuerdo y basado en los objetivos, cada una tiene su origen en cada uno de los objetivos específicos.

Variables Conceptuales

Las variables conceptuales son aquellas que contienen una definición real, es decir, definiciones de diccionarios, libros o fuentes que se especializan en describir la esencia y características de una variable, objeto o fenómeno. Adecúan la definición conceptual a los requerimientos de una investigación. También esta es considerada un tipo de definición técnica.

Variables Operacionales

Las variables operacionales son aquellas que constituyen un conjunto de procedimientos que finalmente describen las actividades que se deben realizar por un observador, el investigador entre otros, para recibir cualquier percepción que indique la existencia de un concepto teórico, en otras palabras, esta variable especifica qué actividades u operaciones se deben realizar para medir una variable, nos indica qué se debe hacer para recolectar los datos necesarios para definir dicha variable, por ejemplo, la definición operacional de una variable temperatura, sería el termómetro.

Estas variables buscan dar claridad o definir la forma en la que se confeccionará los instrumentos con los que se recolectará la información que definirán las variables que responden a nuestros objetivos.

Variables Instrumentales

Una variable instrumental en el contexto de la investigación es un elemento esencial que actúa como el medio o instrumento para la recolección de datos sobre una variable conceptual específica. Mientras que las variables conceptuales representan ideas constructos teóricos que el investigador está interesado en estudiar, las variables instrumentales son las herramientas prácticas que se utilizan para medir o cuantificar esas ideas.

La selección y definición adecuada de las variables instrumentales es crucial para la validez y fiabilidad de cualquier estudio. Es fundamental que estas variables estén claramente definidas y sean capaces de capturar de manera precisa y objetiva la información relevante relacionada con la variable conceptual que se está investigando. Además, deben diseñarse de manera que minimicen los sesgos y errores potenciales en la recolección de datos, garantizando así la integridad y la calidad de los resultados de la investigación.

Tabla 9

Unidades de Análisis

Objetivo Específico	**Variable**	**Variable Conceptual**	**Variable Operacional**	**Variable Instrumental**
Diseñar una infraestructura que facilite el acceso seguro y remoto a la información.	Infraestructura	Según International Business Machines Corporation (IBM, s.f.): "La infraestructura de tecnología de la información, o infraestructura de TI, se refiere al conjunto de componentes necesarios para el funcionamiento y la gestión de los servicios empresariales de TI y entornos de TI."	Entrevista Observación	Guía de Entrevistas Guía de observación

Objetivo Específico	Variable	Variable Conceptual	Variable Operacional	Variable Instrumental
Definir roles y permisos, segmentando y restringiendo el acceso, asegurando la confidencialidad, integridad y disponibilidad de los datos.	Roles Permisos	Según (Entrust, 2023): "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)."	Entrevista	Guía de Entrevistas
Diseñar un plan para que se implemente el teletrabajo conforme a las directrices de ISO/IEC 27018 y NIST SP 800-46	Plan	De acuerdo con (Lara, 2024): "Un plan es un conjunto de pasos, procesos o acciones que se tomarán en el futuro para lograr algunas metas deseadas. La acción del plan está orientada al futuro y la forma de lograrlo se determina de antemano."	Observación	Guía de Observación
Establecer normativas para lograr una configuración uniforme de la seguridad en todos los dispositivos, tomando como guía las directrices de NIST SP	Normativas Configuración de Seguridad	Según la Real Academia Española (RAE, 2024) es el conjunto de normas aplicables a una determinada materia o actividad. De acuerdo con (Cisco, 2024) la configuración de seguridad	Entrevista	Guía de Entrevistas

Objetivo Específico	Variable	Variable Conceptual	Variable Operacional	Variable Instrumental
800-53 e ISO/IEC 27001.		informática es la práctica de proteger sistemas, redes y programas de ataques digitales.		
Diseñar estrategias prácticas para la realización regular de copias de seguridad de datos críticos, en concordancia con las normas ISO/IEC 27031 e ITIL.	Estrategias	Según (Westreicher, 2024): "La estrategia es el plan de acci[on que se disela para poder alcanzar una meta o con un objetivo específico."	Entrevista	Guía de Entrevistas

Fuente: Elaboración Propia

Instrumentos de Recolección de Datos

En el ámbito de la investigación, la recolección de datos es un proceso fundamental que permite obtener la información necesaria para responder a preguntas de investigación y alcanzar los objetivos planteados. Los instrumentos de recolección de datos desempeñan un papel crucial en este proceso, ya que son las herramientas específicas utilizadas para recabar información de manera sistemática y estructurada.

Los instrumentos de recolección de datos pueden adoptar diversas formas y enfoques, dependiendo del tipo de datos que se pretenda obtener y de la metodología de investigación utilizada. Desde cuestionarios y entrevistas hasta observaciones y análisis de documentos, estos instrumentos están diseñados para capturar datos de manera precisa y confiable.

La Observación

Cuando se utiliza el método de observación para la recolección de datos, el mismo implica que sea de corte descriptivo, en otras palabras, el resultado que obtenemos al realizar este método es la descripción de conductas del objeto en estudio. Esta descripción, más adelante se convierte en datos que posteriormente se transforma en evidencia, que respaldará el estudio y los resultados de la investigación. Toda información relevante debe ser registrada para su posterior análisis.

Para decidir cuándo se debe utilizar este método de observación como método de recolección de datos, se aconseja que sea cuando se quiere captar un comportamiento o situación en su contexto natural. Para investigaciones que requieran un enfoque cualitativo, cuando se desea evitar la influencia del investigador en los resultados y para obtener una visión completa y cercana a la realidad de un fenómeno en estudio.

Existen tres tipos de observación, la participante, que es en la que el investigador se involucra en la comunidad, grupo o fenómeno que se está estudiando. No participante, el investigador observa sin interactuar con el grupo, fenómeno u objeto en estudio. Finalmente, estructurada, donde el investigador cuenta con una lista específica de comportamientos o eventos que está buscando, este se explica mejor como en caso de un tipo de auditor.

Algunas pautas para llevar a cabo correctamente la observación como instrumento de recolección de datos son: definir los objetivos, qué se desea aprender con esta observación, seguidamente seleccionar alguno de los tipos anteriormente mencionados, si será participante, no participante o un enfoque estructurado, se debe registrar cada detalle de lo que se observa, para poder analizar esta información a profundidad, más adelante y finalmente interpretar los hallazgos, con base en los datos extraídos, se debe extraer para sacar conclusiones concretas o que nos acerquen a la meta de la investigación.

La Entrevista

La entrevista es un instrumento de recolección de datos, en su mayoría cualitativos, se le permite a los individuos explicar con sus propias palabras, cómo comprenden o interpretan cualquier factor del que deseamos reunir más información. Es aconsejable utilizar estas cuando se busca entender las experiencias personales de los individuos que se ven involucrados en el objeto o fenómeno en estudio.

Existen tres tipos de entrevistas, dentro de los que se consideran los siguientes: entrevistas estructuradas, estas siguen un guion estricto y todas las preguntas se hacen de la misma forma a todos los participantes. Entrevista semiestructurada, esta cuenta con preguntas predefinidas, sin embargo, el entrevistador tiene la libertad de hacer algunas preguntas de seguimiento. Finalmente, contamos con las no estructuradas, son más similares a una conversación libre entre el entrevistador y el entrevistado, y suelen cambiar su enfoque constantemente, las preguntas que aparecen salen con base a las respuestas del entrevistado.

Algunas pautas para emplear correctamente este instrumento para la recolección de datos son, fundamental preparar un conjunto de preguntas en la que se estará enfocando principalmente la conversación, es crucial escuchar activamente a la persona entrevistada y realizar preguntas de seguimiento basadas en sus respuestas si así se requiere. Es esencial hacer sentir cómoda a la persona entrevistada y ser sensible al captar los problemas de la situación que se comenta y por último, registrar y analizar todos los datos de manera sistemática, con la finalidad de no perder detalle alguno.

Proceso para la Recolección y Análisis de Datos

El proceso para la recolección y análisis de datos en una investigación cualitativa es fundamental para obtener resultados significativos y comprensivos. En este estudio, se emplearán dos métodos de recolección de datos clave: entrevistas y observación.

El proceso de recolección de datos se complementará con un riguroso análisis cualitativo. Este análisis implica la identificación de temas, patrones y relaciones emergentes a partir de los datos recopilados. Se emplearán técnicas como el análisis de contenido y la codificación temática para organizar e interpretar la información obtenida de las entrevistas y observaciones.

A través de este proceso integrado de recolección y análisis de datos, se busca alcanzar una comprensión profunda del fenómeno de estudio, permitiendo así la generación de conclusiones significativas y la formulación de recomendaciones pertinentes.

Se debe determinar con los participantes, específicamente Los Gerentes de la empresa CORGIA Gestión e Ingeniería Alternativa, quienes toman las decisiones definitivas de las operaciones empresariales. Para garantizar fiabilidad de los datos recolectados, se estará entrevistando ambos gerentes por separado, sin embargo, aplicando los mismos instrumentos.

Mediante la herramienta de observación se estará comprobando la infraestructura y utilidad diaria que se le da a los equipos en la empresa, así como las limitaciones que serán fácilmente comprobables. Posteriormente se analizarán dichos datos recolectados, y se analizarán las propuestas y proformas más convenientes para elección de la empresa, en conjunto con la sugerencia del investigador.

CAPÍTULO IV: ANÁLISIS DE RESULTADOS

En el capítulo de análisis de resultados se presentan los hallazgos principales que se obtienen de los métodos aplicados para recopilar y analizar la información, específicamente para esta investigación se utilizaron la entrevista y la observación, cuyas respectivas guías se encuentran en los apéndices. De la misma manera, se entiende que uno los objetivos principales de dicha sección consisten en desglosar los datos en frases que denoten la importancia para las preguntas de la investigación, un ejemplo de esto será responder a la pregunta de, qué encontró el investigador.

Algunas características que es importante señalar en esta sección de resultados es que da la oportunidad de resumir los datos en forma de estadísticas descriptivas, lo que nos permite informar al lector de los hallazgos de los análisis así como su correcta interpretación que tiene como finalidad apoyar la hipótesis que se desea realizar, en el caso de esta investigación se basa en la creación de un SGSI (sistema de gestión de seguridad de la información) para que la empresa pueda crear políticas que le permita estar en regla con los referentes internacionales ISO 27001 y su cumplimiento estricto ante una posible auditoría.

Los resultados presentan el producto que se ha conseguido a partir de los datos recolectados mediante los instrumentos que se definieron en la sección anterior, en conjunto con la gerencia de la empresa. Esta sección de la misma manera se apoya en recursos, no precisamente textuales, como la implementación de ser posible, de tablas, gráficos o números que nos permita respaldar y mostrar de forma visual lo que se ha obtenido. Al ser una investigación cualitativa, se entiende que los reportes cualitativos son más flexibles, estos se realizan mediante un esquema narrativo. De igual manera se debe fundamentar las estrategias que han sido utilizadas para abordar el planteamiento, así como los datos que fueron recolectados, analizados e interpretados por el investigador.

Para el análisis de resultados de esta investigación, se han agrupado los resultados obtenidos en los objetivos que se han definido, estos como resultado de la entrevista con los gerentes de la empresa CORGIA Gestión e Ingeniería Alternativa, en función de los objetivos específicos de la investigación, los mismos se resumen a continuación.

Entrevista

En cuanto al diseño de la infraestructura que facilite el acceso seguro y remoto a la información, siguiendo los lineamientos de ISO/IEC 27001 y las prácticas recomendadas de ITIL, se identificaron los siguientes puntos:

Identificación de activos y evaluación de riesgos

Los activos críticos de información identificados por la empresa incluyen principalmente el correo electrónico y algunas bases de datos con información confidencial. Sin embargo, no existe una categorización formal de estos activos. De acuerdo con el Capítulo 4 de la ISO 27001, se debe conocer el contexto de la organización, lo que conlleva: Comprender la organización y su contexto, las expectativas de las partes interesadas, el alcance del SGSI y el SGSI como tal.

La empresa no utiliza una metodología formal para evaluar y gestionar los riesgos de seguridad de la información. La revisión manual se propone como una opción, pero no se ha implementado. En este apartado, se deberá trabajar de acuerdo con el Capítulo 8 de la ISO 27001, el mismo se enfoca en Operación, lo que engloba la planificación operacional y control, el análisis de riesgos de seguridad de la información y el tratamiento de riesgos de seguridad de la información. Para dicha evaluación de riesgos se debe contemplar la fórmula Probabilidad X Impacto = Riesgo. Una vez se conocen los resultados de esta, se pueden catalogar en una tabla de gestión de riesgos de menor impacto hasta crítico.

Políticas y procedimientos

No han establecido políticas y procedimientos formales para la gestión de la seguridad de la información en la organización. La falta de estas políticas puede ser un factor de riesgo importante, el mismo incumple con el Capítulo 5 de la ISO 27001, en este capítulo se contempla el liderazgo y el compromiso, política, funciones, responsabilidades y autoridades de la organización.

De acuerdo con la definición de roles y permisos, segmentando y restringiendo el acceso, asegurando la confidencialidad, integridad y disponibilidad de los datos, se ha identificado:

Gestión de accesos y control de usuarios

El acceso a la información crítica se gestiona mediante una carpeta compartida a la que tienen acceso a través de la red local. No se utilizan sistemas de gestión de identidades y accesos (IAM) para administrar los privilegios de acceso. No hay un control riguroso sobre quién tiene acceso a qué información, lo que puede aumentar el riesgo de exposición de datos sensibles. Ambos nos llevan al Capítulo 7 de la ISO 27001. Este capítulo se enfoca en Soporte, y uno de los principales temas es sobre los recursos, la organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información.

Protección contra malware y respaldo de la información

Utilizan software antivirus AVG en las computadoras para mitigar riesgos de seguridad. Sin embargo, no cuentan con un sistema centralizado de gestión de seguridad de la información. La infraestructura actual consiste en un servidor de archivos con sistema operativo Windows 8.1 Pro y un disco duro externo para respaldos. Realizan copias automáticas incrementales en un disco externo, pero no tienen un sistema centralizado de copias de seguridad ni políticas formales para la gestión de activos de información.

Para estos apartados, se continúa en el capítulo 7 de la Norma ISO 27001, que incluso nos indica sobre la importancia de la información documentada que requiere el sistema de gestión de la información. En conjunto con el Capítulo 8, que nos describe que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información y para implementar las acciones determinadas en el apartado 6.1 (acciones para tratar riesgos y oportunidades).

Relacionado al diseño de un plan para que se implemente el teletrabajo conforme a las directrices de ISO/IEC 27018 y NIST SP 800-46, se pudo determinar que:

Formación y concienciación

No proporcionan formación regular sobre seguridad de la información a los empleados. La falta de conciencia y capacitación puede aumentar el riesgo de incidentes de seguridad. En el

capítulo 7 de Soporte de la Norma ISO 27001, se establece el apartado de competencia, en el que la formación, capacitación, experiencia y educación del personal, debe de ser contemplado en el SGSI. Así como el apartado de concientización, indica que un personal consciente de la política, contribución al SGSI conoce las implicaciones ante el incumplimiento, las cuales se deben de establecer de igual manera. Finalmente, la comunicación, en este mismo apartado se solicita a la organización, que debe determinar la necesidad de comunicaciones internas y externas pertinentes al SGSI que se implementará.

Gestión de incidentes de seguridad

No tienen un proceso establecido para manejar incidentes de seguridad de la información. La falta de protocolos claros puede dificultar la respuesta efectiva a amenazas de seguridad. Es requerido realizar en el Capítulo 8 de Operación de la Norma ISO 27001, una tabla con la probabilidad de ocurrencia, que va desde raro, improbable, posible, probable y casi seguro, de acuerdo con su frecuencia. Y colocar dichos eventos en una matriz de calificación, evaluación y respuesta a los riesgos, en esta se catalogan también con un impacto que va desde insignificante, menor, dañino, severo y crítico. Las respuestas de las intersecciones de dicha matriz, nos resulta en las categorías finales en la que se deben categorizar dichos eventos y a la vez la criticidad de la información en cuestión. Finalmente, estas zonas y su respuesta de riesgo ante un posible incidente se catalogan como se muestra en la Figura 1:

Figura 1

Tabla Calificación, Evaluación y Respuesta a los Riesgos

B	Zona de Riesgo Baja	Asumir el riesgo
M	Zona de Riesgo Moderada	Asumir el riesgo, evaluar, reducir el riesgo
A	Zona de Riesgo Alta	Reducir rel riesgo, evitar, compartir o transferir
E	Zona de Riesgo Extrema	Reducir el riesgo, evitar, compartir o transferir

Fuente: Elaboración Propia, 2024

En cuanto al establecimiento de normativas para lograr una configuración uniforme de la seguridad en todos los dispositivos, se obtuvieron los siguientes hallazgos:

Auditorías y revisiones

No se han realizado auditorías internas periódicas para verificar el cumplimiento de las políticas de seguridad de la información. La ausencia de estas revisiones puede dificultar la identificación de áreas de mejora y el mantenimiento de un nivel adecuado de seguridad.

Esto contempla un apartado muy importante para nuestro SGSI, en el Capítulo 9 de la Norma ISO 27001 se detalla la evaluación del desempeño, en la que se contempla el seguimiento, medición, análisis y evaluación, así como incluir las auditorías internas y una revisión por la dirección. En la evaluación del desempeño, se programan las auditorías internas, se debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión, mediante la medición de la eficacia de los controles, una revisión de las evaluaciones y tratamientos de riesgo, seguimiento y revisión de los procedimientos de detección y prevención de incidentes y una actualización de los planes.

Finalmente, relacionado al diseño de estrategias prácticas para la realización regular de copias de seguridad de datos críticos, se enumeran las siguientes observaciones:

Protección de datos

Aunque realizan copias automáticas incrementales en un disco externo, no cuentan con un sistema centralizado de copias de seguridad ni políticas formales para la gestión de activos de información. Esta falta de estructura puede resultar en la pérdida de datos críticos en caso de un incidente de seguridad o un fallo del sistema.

Mejora continua

La empresa debe desarrollar e implementar políticas formales para la gestión de copias de seguridad que establezcan procedimientos claros y regulares para la realización y verificación de copias de seguridad. Además, es importante realizar análisis posteriores a incidentes para identificar áreas de mejora en el proceso de copias de seguridad. De acuerdo con el Capítulo final de la Norma ISO 27001, el capítulo de mejora se especifica, de acuerdo con el análisis que se ha realizado, que la organización debe continuamente mejorar la adecuación, sostenimiento y efectividad del SGSI. No debe haber conformidades, más sí acciones correctivas, es decir, es imperativo reaccionar ante la no conformidad, evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir, ni ocurra en otra parte. Implementar cualquier acción que se considere necesaria, revisar la eficacia de las acciones correctivas llevadas a cabo y finalmente, si es necesario, hacer cambios al SGSI.

Observación

Dinámica de trabajo remoto: La mayoría de las labores pueden realizarse de manera efectiva de forma remota, lo que sugiere una oportunidad para implementar procesos virtuales en línea con las pautas de ISO/IEC 27001:2022 y COBIT 2019. Sin embargo, es importante considerar la necesidad de establecer políticas y procedimientos formales para garantizar la seguridad y confidencialidad de la información durante estas actividades.

Identificación de tareas críticas: Se observa que actualmente cualquier dispositivo con acceso a la red local puede ingresar a cualquier información en el servidor central. Esta falta de segregación de usuarios, roles y privilegios representa un riesgo de seguridad significativo y destaca la necesidad urgente de implementar medidas adicionales para proteger los datos sensibles de la empresa.

Factibilidad de tareas remotas: Aunque no fue posible observar la diversidad completa de tareas durante la visita, es importante identificar y analizar las actividades que no son factibles de realizar de forma remota, tales como los estudios eléctricos, estos se realizan a campo. Esto permitirá ajustar o mitigar su impacto en la operación de acuerdo con los requisitos de continuidad del negocio establecidos en ISO/IEC 27001:2022.

Infraestructura de red: La infraestructura actual es limitada pero adecuada para el tamaño actual de la empresa. Sin embargo, se requiere una planificación cuidadosa para migrar a una nueva infraestructura que admita el teletrabajo de manera segura, especialmente considerando la necesidad de clasificar adecuadamente la información y garantizar la seguridad de la transmisión de datos.

Seguridad de dispositivos: Aunque se cumplen algunas medidas de seguridad para el correo electrónico, como lo es la autenticación Multifactorial, también que las contraseñas son únicamente manejadas por la gerencia, por lo que se imposibilita a los empleados abrir una sesión en cualquier otro dispositivo que no sea empresarial; es evidente la necesidad de implementar medidas adicionales en otros aspectos de la empresa para cumplir con las directrices de seguridad de la información de ISO/IEC 27002. Esto incluye la autenticación de usuarios y la gestión de parches en todos los dispositivos utilizados para el trabajo remoto.

Identificación de amenazas y vulnerabilidades: Aunque no se han identificado riesgos adicionales más allá de los comúnmente asociados con el uso de Internet, es crucial seguir monitoreando y evaluando constantemente las posibles amenazas y vulnerabilidades asociadas con el teletrabajo. Esto garantizará una respuesta proactiva y efectiva en caso de incidentes de seguridad.

Este análisis de resultados proporciona una visión detallada de los aspectos observados durante la evaluación de la capacidad de la empresa para implementar el trabajo remoto de manera segura y efectiva. Identifica áreas críticas que requieren atención inmediata y ofrece recomendaciones específicas para mejorar la seguridad de la información y garantizar la continuidad del negocio.

Resumen

La empresa CORGIA Gestión e Ingeniería Alternativa carece de políticas y procedimientos formales para la gestión de la seguridad de la información, lo que representa un riesgo significativo para la confidencialidad, integridad y disponibilidad de los datos, la misma presenta deficiencias significativas en la gestión de la SI, incluida la falta de políticas formales, evaluación de riesgos y gestión de incidentes, que son cruciales en un SGSI.

- Según el análisis realizado, se requiere desarrollar un SGSI desde cero, lo que significa que se deben contemplar todos y cada uno de sus pasos para su implementación, incluyendo la creación de políticas y procedimientos formales basados en estándares como ISO/IEC 27001, ISO/IEC 27002 para mejorar la gestión de la seguridad de la información y garantizar su integridad, disponibilidad y confidencialidad.
- Es fundamental realizar un plan para proporcionar formación regular sobre seguridad de la información a los empleados.
- De igual manera se identifica como crítico no contar con un proceso formal para manejar incidentes de seguridad, de acuerdo con la situación actual de la empresa, incluso desconocer los posibles incidentes a los que se pueden enfrentar, al desconocer el tipo de información que manejan y su criticidad, incluso exponerse a un incidente en el que no se puede medir su impacto.

Este análisis completo proporciona una visión integral de la situación actual de la empresa CORGIA Gestión e Ingeniería Alternativa en cuanto a la gestión de la seguridad de la información, incluyendo aspectos como identificación de activos, gestión de riesgos, políticas y procedimientos, gestión de accesos, protección contra malware, formación y concienciación, gestión de incidentes, auditorías y revisiones, entre otros. La investigación, de acuerdo al análisis realizado, se centra en la necesidad de desarrollar e implementar políticas y procedimientos formales, proporcionar formación regular a los empleados y establecer procesos para la mejora continua y la adaptación a los cambios en el entorno de amenazas, todo esto incluido en un Sistema de Gestión de Seguridad de la Información.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Se ha identificado que la dependencia de un servidor físico local constituye una limitación significativa para la empresa CORGIA Gestión e Ingeniería Alternativa. Esta situación restringe el acceso remoto y la flexibilidad laboral, impactando negativamente en la eficiencia operativa, por lo que se logró diseñar con éxito una infraestructura de acceso seguro y remoto que cumple con los estándares de ISO/IEC 27001 y las mejores prácticas de ITIL. Esta infraestructura mejora significativamente la accesibilidad y seguridad de la información, permitiendo a la empresa operar de manera más eficiente y segura en un entorno digital.

La falta de partición de información y la ausencia de protocolos de seguridad adecuados aumentan los riesgos de acceso no autorizado y comprometen la confidencialidad de los datos, para esto se ha definido y documentado exitosamente un sistema de roles y permisos que segmenta y restringe el acceso a la información según las funciones específicas de los usuarios. Esto asegura la confidencialidad, integridad y disponibilidad de los datos, garantizando que solo los usuarios autorizados accedan a la información necesaria para sus roles.

En un contexto donde la movilidad y la flexibilidad son esenciales, la falta de acceso remoto y protocolos de seguridad adecuados impide la implementación efectiva del teletrabajo. Esto no solo podría afectar la continuidad operativa de la empresa, sino también la retención de talento clave, subrayando la necesidad urgente de establecer una infraestructura tecnológica robusta y segura, consecuentemente se diseñó un plan de teletrabajo que cumple con las directrices de ISO/IEC 27018 y NIST SP 800-46. Este plan proporciona un marco seguro para el trabajo remoto, aumentando la flexibilidad laboral y la satisfacción de los empleados, al tiempo que protege los datos y sistemas de la empresa.

La carencia de una configuración uniforme de seguridad en los dispositivos y la falta de un sistema eficiente de respaldo en la nube ponen en riesgo tanto la integridad como la continuidad del negocio de CORGIA. Para mitigar estos riesgos y proteger los activos de información, se estableció una guía con un acompañamiento para aplicar con éxito normativas de seguridad

uniformes para todos los dispositivos, basadas en NIST SP 800-53 e ISO/IEC 27001. Esta medida garantiza una configuración de seguridad coherente en toda la organización, reduciendo significativamente los riesgos de seguridad y mejorando la protección de los activos de información.

La falta de copias de seguridad regulares exponía a la organización a la pérdida permanente de información crítica, ya sea por fallos en el sistema, errores humanos o ataques cibernéticos, afectando la integridad, para garantizar la continuidad del negocio, se ha desarrollado una guía con estrategias de copias de seguridad basadas en ISO e ITIL. Estas estrategias aseguran la protección de datos críticos y la capacidad de restauración rápida en caso de pérdida de datos, mejorando su capacidad de recuperación ante desastres y reforzando la protección de sus activos de información.

Las limitaciones de esta investigación incluyen la dependencia de datos secundarios y la variabilidad en la implementación de medidas de seguridad, que abarcan aspectos como roles específicos, permisos, la frecuencia de aplicación de políticas de seguridad, herramientas utilizadas, tipos de información manejada y su criticidad. Estos aspectos son internos a la empresa y deben ser definidos por CORGIA para aplicar adecuadamente las políticas y controles sugeridos, considerando que ciertos detalles se mencionan de manera general en las guías consultadas.

Recomendaciones

Implementación de una Infraestructura de Acceso Remoto y Seguro: Para mejorar la accesibilidad y seguridad de la infraestructura, se recomienda implementar un plan de migración hacia una infraestructura más moderna. Este plan incluirá el uso de herramientas avanzadas como autenticación multifactor, O365, y VPN. Debe de realizarse por los gerentes de la empresa en conjunto con el equipo de TI en el primer trimestre del siguiente año fiscal de la empresa, se estima una duración del primer cuarto del año para migrar completamente, con un costo aproximado de $425 en licencias anuales y $12.50 mensuales por usuario de Office 365.

Gestión de Seguridad de la Información: Es crucial establecer políticas documentadas de seguridad de la información, en conformidad con las normativas internacionales. Esto se logrará mediante la creación y difusión del Manual de Políticas de Seguridad que detalla roles, permisos

y protocolos de acceso a la información. La implementación se realizará previo al despliegue de las nuevas tecnologías, en el último cuarto del año fiscal en curso, asegurando la formación y aceptación del personal, el principal responsable es el departamento de gerencia y su duración es aproximadamente de un trimestre pasando por todas sus etapas de revisión.

Uniformidad en la Configuración de Seguridad de los Dispositivos: Se recomienda establecer estándares de seguridad consistentes basados en las normativas internacionales para todos los dispositivos. Esto incluye la definición de procedimientos para la instalación de antivirus, configuraciones de cortafuegos y otras medidas esenciales. La implementación será simultánea con la infraestructura de acceso remoto seguro, este esfuerzo deberá ser en conjunto de la gerencia y el departamento de TI, su duración se extenderá según la integración de la nueva infraestructura.

Desarrollo de un Plan de Respaldo y Recuperación de Datos en la Nube: Para garantizar la continuidad del negocio, se recomienda desarrollar una guía detallada con estrategias de copias de seguridad basadas en los estándares internacionales. Esta guía incluirá procedimientos para la segmentación de datos y pruebas de restauración, asegurando la protección de datos críticos. La implementación será posterior a la migración de la información a la infraestructura de acceso remoto seguro, este esfuerzo deberá ser en conjunto de la gerencia y el departamento de TI, se estima una duración de dos semanas para tener un sistema de respaldo funcional y probado en todas sus etapas, la misma se puede extender según los resultados de las pruebas a realizar para garantizar su completa funcionalidad.

Gestión de Incidentes y Auditorías Internas Es esencial establecer un manual para la gestión de incidentes y la planificación de auditorías internas, basado en la normativa ISO/IEC 27001. Se sugiere la implementación de un manual que detallará procedimientos para la identificación, respuesta y mitigación de incidentes, así como la ejecución de auditorías regulares. Misma a realizar posterior a la integración de la infraestructura sugerida, una vez identificados los posibles riesgos, y posterior a la categorización de la información en niveles de criticidad. Este esfuerzo es coordinado por la gerencia, su duración aproximada es de un cuarto del año, misma que podrá extenderse según las prácticas de respuesta a incidentes que se identifican.

Capacitación y Concienciación en Seguridad de la Información: Se recomienda desarrollar un programa continuo de formación y concienciación en seguridad de la información, basado en ISO/IEC 27001. Este programa incluirá capacitación en políticas de seguridad, manejo de datos y concienciación sobre amenazas y mejores prácticas. Se implementará de forma continua, con evaluaciones semestrales para actualizar el contenido conforme a nuevas amenazas y tecnologías emergentes. Su implementación es simultánea a la integración de los manuales que conforman esta propuesta integral, de esta manera el personal estará capacitado a la correcta utilización de las herramientas y el correcto manejo de la información, una vez se implementen de manera proactiva, este esfuerzo debe coordinarlo la gerencia de la organización. Su duración es indefinida, ya que es un programa continúo con evaluaciones semestrales, anuales entre otros.

REFERENCIAS

AGV Antivirus. (2024). *Support for Windows Products*. Obtenido de AGV Support: https://support.avg.com/support_win?l=en

ASANA. (8 de Enero de 2023). *¿Quiénes son los stakeholders de un proyecto? Descubre cómo identificarlos y gestionarlos para asegurar el éxito del proyecto*. Obtenido de asana.com: https://asana.com/es/resources/project-stakeholder

AWS. (2023). *¿Qué es la transformación digital?* Obtenido de aws.amazon.com: https://aws.amazon.com/es/what-is/digital-transformation/

Axelos. (2024). *The framework for the management of IT-enabled services*. Obtenido de ITIL: https://www.axelos.com/certifications/itil-service-management

Bungee, M., & Ardilla, R. (2002). *Filosofía de la psicología.* México: Siglo XXI Editores (2.ª ed.).

CFIA. (07 de Noviembre de 2023). *Colegio Federado de Ingenier[ia y de Arquitectos de Costa Rica*. Obtenido de Quienes Somos: https://cfia.or.cr/quienesSomos.html

Chapple, M. (2019). *Understanding Firewall Fundamentals*. Obtenido de Lifewire: https://www.lifewire.com/what-is-a-firewall-2487290

Cisco. (2024). *¿Qué es la seguridad de red?* Obtenido de cisco.com: https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html

Cisco Networking. (2019). *Redes Empresariales*. Obtenido de Cisco.com: https://www.cisco.com/c/dam/global/es_mx/solutions/small-business/pdfs/smb-redes-mx.pdf

Comillas Universidad Pontificia. (8 de Mayo de 2023). *Confidencialidad, Integridad y Disponibilidad*. Obtenido de ciberseguridad.comillas.edu: https://ciberseguridad.comillas.edu/confidentiality-integrity-and-availability/

Dhillon, G., & Moores, T. (2001). Computer Security Incident Handling Step by Step. En *Information Security Management Handbook* (págs. 25-30).

Editorial Equipo. (14 de 11 de 2023). *Significados.com.* Obtenido de "Qué es Hardware": https://www.significados.com/hardware/

Entrust. (2023). *¿QUÉ ES EL CONTROL DE ACCESO BASADO EN ROLES (RBAC)?* Obtenido de entrust.com: https://www.entrust.com/es/resources/faq/what-is-role-based-access-control

IBM. (s.f.). *¿Qué es el almacenamiento de datos?* Obtenido de ibm.com: https://www.ibm.com/es-es/topics/data-storage

IBM. (s.f.). *¿Qué es infraestructura de TI?* Obtenido de ibm.com: Definir roles y permisos, segmentando y restringiendo el acceso, asegurando la confidencialidad, integridad y disponibilidad de los datos

IBM. (s.f.). *¿Qué es la recuperación de datos?* Obtenido de ibm.com: https://www.ibm.com/es-es/topics/data-recovery

Internation Standard ISO 22301. (Octubre de 2019). *Security and resilience Business continuity management systems Requirements.* Obtenido de cdn.standards:

https://cdn.standards.iteh.ai/samples/75106/d11801a9bab045a88d59cd321519ecf1/ISO-22301-2019.pdf

IONOS. (30 de Mayo de 2022). *Tipos de copia de seguridad: resumen de los principales métodos y estrategias*. Obtenido de Digital Guide Ionos: https://www.ionos.es/digitalguide/servidores/know-how/tipos-de-copias-de-seguridad/

ISACA Costa Rica Chapter. (2019). *ISACA Capítulo Costa Rica*. Obtenido de https://www.isacacr.org/

John W, C. (2009). *Research Design Qualitative, Quantitative, and Mixed Methods Approaches.* Nebraska: SAGE.

KPMG. (2020). *Auditoría y Monitore Continuo.* Obtenido de assets.kpmg.com: https://assets.kpmg.com/content/dam/kpmg/cl/pdf/2020-06-kpmg-chile-audit-monitoring.pdf

La Gaceta. (30 de Septiembre de 2019). *LEY PARA REGULAR EL TELETRABAJO* . Obtenido de mtss.go.cr: https://www.mtss.go.cr/elministerio/marco-legal/documentos/9738.pdf

Lara, J. M. (2024). *¿QUÉ ES UN PLAN? DEFINICIÓN, CARACTERÍSTICAS Y PASOS*. Obtenido de josemarialara.es: https://www.josemarialara.es/que-es-un-plan-definicion-caracteristicas-y-pasos/

LiFeder. (2024). *Fuentes de información*. Obtenido de lifeder.com: https://www.lifeder.com/fuentes-de-informacion/

Mattord, M. E. (2016). Principles of Information Security. Cengage Learning. En *Principles of Information Security. Cengage Learning.*

Microsoft. (25 de 10 de 2023). *Creación de un plan de seguridad para el acceso a recursos*. Obtenido de Microsoft Learn: https://learn.microsoft.com/es-es/entra/architecture/3-secure-access-plan

Microsoft. (21 de 08 de 2023). *Introducción a la administración del acceso con privilegios*. Obtenido de Microsoft Learn: https://learn.microsoft.com/es-es/purview/privileged-access-management-configuration

Microsoft. (2024). *¿Qué es la seguridad de la información (InfoSec)?* Obtenido de microsoft.com: https://www.microsoft.com/es-co/security/business/security-101/what-is-information-security-infosec

Microsoft. (09 de 04 de 2024). *Administración del acceso de usuarios y usuarios invitados con revisiones de acceso*. Obtenido de Microsoft Learn: https://learn.microsoft.com/es-es/entra/id-governance/manage-access-review

Microsoft. (2024). *Dejar de compartir archivos o carpetas de OneDrive o SharePoint o cambiar los permisos*. Obtenido de Microsoft Support: https://support.microsoft.com/es-es/office/dejar-de-compartir-archivos-o-carpetas-de-onedrive-o-sharepoint-o-cambiar-los-permisos-0a36470f-d7fe-40a0-bd74-0ac6c1e13323

Microsoft. (2024). *Usar Microsoft Authenticator con Microsoft 365*. Obtenido de Microsoft Support: https://support.microsoft.com/es-es/topic/usar-microsoft-authenticator-con-microsoft-365-1412611f-ad8d-43ab-807c-7965e5155411

Microsoft. (2024). *Usar Microsoft Authenticator con Microsoft 365*. Obtenido de Microsoft Support: https://support.microsoft.com/es-es/topic/usar-microsoft-authenticator-con-microsoft-365-1412611f-ad8d-43ab-807c-7965e5155411

Microsoft Corporation. (25 de 10 de 2023). *Niveles de permisos y permisos de usuario de SharePoint Server local*. Obtenido de Microsoft Learn: https://learn.microsoft.com/es-es/sharepoint/sites/user-permissions-and-permission-levels

Microsoft Corporation. (2024). *Crear una carpeta en una biblioteca de documentos*. Obtenido de Microsoft Support: https://support.microsoft.com/es-es/office/crear-una-carpeta-en-una-biblioteca-de-documentos-3d6a8c11-2490-4d6b-8837-f25649a69c56

Microsoft Corporation. (2024). *Usar Microsoft Authenticator con Microsoft 365*. Obtenido de Microsoft Support: https://support.microsoft.com/es-es/topic/usar-microsoft-authenticator-con-microsoft-365-1412611f-ad8d-43ab-807c-7965e5155411

Microsoft Support. (22 de 02 de 2024). *Set up multifactor authentication for Microsoft 365*. Obtenido de Microsoft Learn: https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide

Ministerio de Trabajo y Seguridad Social. (Junio de 2020). *POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN* . Obtenido de mtss.go.cr: https://www.mtss.go.cr/perfiles/lineamientos_circulares_directrices_politicas_internas/lineamientos-circulares-directrices-politicas%20internas/DGAF-DTIC-OF-191-2020.pdf

Nagios. (s.f.). *Notifications*. Obtenido de Nagios Core: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/notifications.html

Nagios. (s.f.). *Quickstart Installation Guides*. Obtenido de Nagios Core: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/quickstart.html

NIST. (Julio de 2016). *NIST SP 800-46 Rev. 2*. Obtenido de NIST Information Technology Laboratory: https://csrc.nist.gov/pubs/sp/800/46/r2/final

NOATICA. (2023). *ISO/IEC 27002: La Guía para las buenas prácticas en Seguridad de la Información*. Obtenido de noatica.com: https://noatica.com/iso-iec-27002/

NormasISO. (2005). *ISO 27001 SEGURIDAD DE LA INFORMACIÓN*. Obtenido de normas-iso.com: https://www.normas-iso.com/iso-27001/

Pearson, S. (2013). En *Privacy, Security and Trust in Cloud Computing.* Springer.

Pfleeger, C. P., & Pfleeger, S. L. (2012). En *Security in Computing.* Pearson Education.

RAE. (2024). *normativo, va*. Obtenido de dle.rae.es: https://dle.rae.es/normativo?m=form

Roesch, M. (1999). *Snort - LightWeight Intrusion Detection For Networks*. Obtenido de https://www.usenix.org/legacy/publications/library/proceedings/lisa99/full_papers/roesch/roesch.pdf

Sampieri, R. H., Valencia, S. M., Torres, C. P., & Romo, A. C. (2017). *Fundamentos de Investigación.* Mexico: Mc Graw Hill Education.

Sistema Costarricense de Información Jurídica. (09 de Febrero de 2024). *ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA.* Obtenido de pgrweb.go.cr:

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=73583

SOLBYTE. (18 de Abril de 2022). *¿Qué es una licencia de software y para qué sirve?* Obtenido de solbyte.com: Licencias de software

Tecnología Mix. (2023). *¿Qué es una infraestructura de red?* Obtenido de tecnologiamix: https://www.tecnologiamix.com/que-es-una-infraestructura-de-red

Tribunal Supremo de Elecciones. (05 de Septiembre de 2011). *LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES Ley n.º 8968.* Obtenido de tse.go.cr: https://www.tse.go.cr/pdf/normativa/leydeprotecciondelapersona.pdf

UNED. (28 de Enero de 2019). *Programa de Teletrabajo*. Obtenido de Universidad Estatal a Distancia: https://www.uned.ac.cr/viplan/teletrabajo/que-es-teletrabajo/que-es-teletrabajo

UNE-EN ISO/IEC 27002. (Mayo de 2017). *Código de prácticas para los controles de seguridad de* . Obtenido de https://www.une.org/

Vallis, D. (Junio de 2017). *An Introduction to Computer Security: The NIST Handbook*. Obtenido de https://csrc.nist.gov/pubs/sp/800/12/r1/final

WatchGuard. (2018). *Acerca de las Reglas y Conjuntos de Reglas*. Obtenido de Fireware Help: https://www.watchguard.com/help/docs/fireware/12/es-419/Content/es-419/proxies/general/rule_rulesets_about_c.html

WatchGuard. (2023). *Instalar el Software Cliente de WatchGuard*. Obtenido de WatchGuard Help Center: https://www.watchguard.com/help/docs/help-center/es-xl/Content/en-US/Endpoint-Security/installation/install-client-software.html?

WatchGuard. (2023). *Acerca de los Algoritmos y Protocolos de IPSec*. Obtenido de WatchGuard Help Center: https://www.watchguard.com/help/docs/help-center/es-xl/Content/en-US/Fireware/mvpn/general/ipsec_algorithms_protocols_c.html

WatchGuard. (2023). *Bloquear Aplicaciones Evasivas*. Obtenido de WatchGuard Help Center: https://www.watchguard.com/help/docs/help-center/es-xl/Content/en-US/Fireware/configuration_examples/block_evasive_apps_example.html

WatchGuard. (2023). *Configurar VPN Administradas*. Obtenido de WatchGuard Help Center: https://www.watchguard.com/help/docs/help-center/es-xl/Content/en-US/Fireware/dimension/managed_vpns_configure_d.html

WatchGuard. (2024). *Configure Firewall Policies in WatchGuard Cloud*. Obtenido de WatchGuard Support: https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/WG-Cloud/Devices/managed/firewall_policies_configure.html

WatchGuard. (2024). *Quick Start Set Up WatchGuard EDR Core*. Obtenido de WatchGuard Support: https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/services/edr_core/edr_core_quick_start_c.html

Westreicher, G. (1 de Septiembre de 2020). *Retorno de la inversión (ROI)*. Obtenido de economipedia.com: https://economipedia.com/definiciones/retorno-de-la-inversion-roi.html

Westreicher, G. (05 de Febrero de 2024). *Estrategia: Qué es, tipos y ejemplos*. Obtenido de economipedia.com: https://economipedia.com/definiciones/estrategia.html#

Whitman, M. E., & Mattord, H. J. (2016). En *Management of Information Security* (pág. 5th ed.). Cengage Learning.

APÉNDICE A

Guía Entrevista a realizar a la empresa CORGIA.

GUÍA DE ENTREVISTA

Entidad:	CORGIA Gestión e Ingeniería Alternativa
Nombre del entrevistado:	Hazel Adriana Mora Mora
Puesto del entrevistado:	Gerente General CORGIA
Nombre del estudiante:	Melannie Angélica Mora Corrales
Fecha de la entrevista:	Mayo 07, 2024
Lugar o medio de la entrevista:	Oficinas CORGIA

Preguntas:

Identificación de activos y evaluación de riesgos:

1. ¿Cómo identifican y categorizan los activos de información críticos para su organización? Actualmente no lo tenemos organizado. Sin embargo, lo único crítico es el correo electrónico, se tiene información confidencial en bases de datos, pero no es información que no es requerida para la continuidad de negocio. Y no contenemos ningún tipo de secretos comerciales.

2. ¿Qué metodología utilizan para evaluar y gestionar los riesgos de seguridad de la información?

No utilizamos ninguna metodología realmente, pero si lo hiciéramos tendríamos que revisar manualmente para identificar cual información es estrictamente confidencial, entre otros. Lo que tenemos es una carpeta compartida a la que tienen acceso por medio de la red local. Actualmente se planifica crear un grupo de hogar para limitar este acceso a únicamente los dispositivos de la empresa.

3. Conforme a la política de gestión de activos de la información según ISO/IEC 27001:2022, ¿podrían especificar el tipo de servidor central utilizado en su infraestructura actual, incluyendo su versión actual y capacidad de almacenamiento? Esta información es esencial para evaluar la adecuación de los activos de TI a los requisitos de seguridad.

Es un servidor de archivos, con una RAM de 8GB, sistema operativo obsoleto Windows 8.1 Pro, de almacenamiento tiene 327 GB de las cuales 44,6GN están disponibles. Contamos con cuentas de correo de Google workspace, en la que generamos copias de seguridad. Nuestra página web está almacenada en go daddy, por lo que no la tenemos local., y tenemos un disco duro externo para los respaldos, no contamos con servidor de copias de seguridad.

4. ¿Podrían proporcionar detalles sobre el número de computadoras en su inventario actual y cualquier información relevante sobre su configuración?

7 laptops que utilizan de sistema operativo Windows 10 Home, las de gerencia utilizan Windows 11 Home, 1 PC y el servidor central.

Políticas y procedimientos:

5. ¿Han establecido políticas y procedimientos formales para la gestión de la seguridad de la información?

No.

6. ¿Cómo se comunican y se hacen cumplir estas políticas en toda la organización?

No aplica, sin embargo, se espera dar instrucciones claras, concisas y con capacitación constante a los empleados.

Gestión de accesos y control de usuarios:

7. ¿Cómo gestionan los accesos de los usuarios a los sistemas y datos sensibles?

Actualmente lo que existe es un acceso en cada computadora a un mismo archivo que está en el servidor en el que se contiene la información de la empresa para realizar sus labores diarias.

8. ¿Utilizan algún sistema de gestión de identidades y accesos (IAM) para administrar los privilegios de acceso?

No, únicamente acceso por dispositivo. Se planifica crear un grupo hogar de momento para garantizar que únicamente las computadoras de la empresa puedan ingresar.

9. Según la política de protección contra malware de ISO/IEC 27002, ¿utilizan algún tipo de software antivirus en las computadoras actuales para mitigar los riesgos de seguridad? La información sobre el tipo de licencia, su precio actual y la modalidad de pago es necesaria para evaluar la efectividad y cumplimiento de las medidas de seguridad.

AVG para 10 dispositivos por 2 años que incluye: AVG Internet Security, AVG TuneUp, AVG Secure VPN y AVG AntiTrack.

10. De acuerdo con la política de respaldo de la información de ISO/IEC 27002, ¿cuentan con algún sistema de respaldo para garantizar la disponibilidad y la integridad de los datos críticos?

Un disco externo que realiza copias automáticas incrementales.

Formación y concienciación:

11. ¿Qué medidas toman para concienciar al personal sobre la importancia de la seguridad de la información?

Se firma un contacto de confidencialidad, en el que, como consecuencia de incumplir, se enfrentar a la terminación de su contrato. Por otra parte, las claves de correo son gestionadas por la gerente únicamente, por lo que no pueden iniciar sesión en otros dispositivos ni cambiar la clave actual.

12. ¿Proporcionan formación regular sobre seguridad de la información a los empleados?

No contamos con la misma, por lo que no se realiza.

Gestión de incidentes de seguridad:

13. ¿Cómo manejan los incidentes de seguridad de la información cuando ocurren?

No han tenido ningún incidente de seguridad. Sin embargo, se espera que sean notificados inmediatamente a los gerentes de la empresa.

14. ¿Tienen establecido un proceso de notificación y respuesta a incidentes?

No, únicamente comunicación directa con la gerencia.

Auditorías y revisiones:

15. ¿Realizan auditorías internas periódicas para verificar el cumplimiento de las políticas de seguridad de la información?

Por el momento no se tienen dichas políticas, pero se espera poder tener auditorías constantes una vez que sean creadas y puestas en marcha.

16. ¿Cómo se llevan a cabo las revisiones de la eficacia del SGSI y se implementan mejoras, si existe un SGSI?

No aplica.

En caso de no contar con un SGSI, saltar a la pregunta 19.

Mejora continua:

17. ¿Qué medidas toman para mejorar continuamente el SGSI y adaptarlo a los cambios en el entorno de amenazas y en los requisitos comerciales?
18. ¿Realizan análisis posteriores a incidentes para identificar áreas de mejora?

Cumplimiento normativo:

19. ¿Cómo aseguran el cumplimiento de las normativas y regulaciones relevantes en materia de seguridad de la información?

Por el momento no, se cuenta con regulaciones ni normativas que garanticen la seguridad de la información.

20. ¿Participan en auditorías externas para validar el cumplimiento de los estándares ISO/IEC 27001 y otros requisitos legales?

No, nunca hemos participado en una auditoría externa.

Gestión de proveedores:

21. ¿Cómo evalúan y gestionan el riesgo de seguridad de los proveedores y socios externos?

No tenemos forma de evaluarlo, recientemente estamos tratando de generar algunas políticas sin embargo se desconoce completamente cómo aplicarlas. Actualmente los proveedores hacen a la empresa firmar contratos de confidencialidad, sin embargo, la empresa a ellos no.

22. ¿Tienen establecidos acuerdos de seguridad de la información con los proveedores?

Sí, tenemos acuerdos de confidencialidad que se firman con los proveedores.

Continuidad del negocio y recuperación ante desastres:

23. ¿Qué medidas tienen implementadas para garantizar la continuidad del negocio en caso de interrupciones o desastres?

Los gerentes contamos con una computadora de respaldo cada uno, que constantemente realizamos copias de seguridad de información selectiva, y contamos con los correos que, podemos acceder desde otras computadoras o en línea en caso de requerir acceso inmediato ante una eventualidad.

24. ¿Se realizan pruebas periódicas de los planes de recuperación ante desastres?

Recientemente realizamos una prueba porque el disco duro externo no estaba haciendo las copias de seguridad, pero no se tiene planificado las pruebas en un plan ni de manera constante.

APÉNDICE B

Guía Observación para realizar a la empresa CORGIA Gestión.

GUÍA DE OBSERVACIÓN

Entidad:	CORGIA Gestión e Ingeniería Alternativa
Dirección física de la entidad:	San Rafael Abajo, Desamparados
Fecha de la actividad de observación:	Mayo 07, 2024
Nombre del estudiante:	Melannie Angélica Mora Corrales

Tabla de control de aspectos observados:

No	Aspectos por observar	Cumple	No Cumple	Oportunidad de mejora	Detalle de Observación
1	Se observa cómo se lleva a cabo la dinámica de trabajo para determinar si existen procesos que puedan realizarse de manera efectiva de forma remota, conforme a las pautas de ISO/IEC 27001:2022 y COBIT 2019.	X			Las labores son básicas, responder correos, atender llamadas, realizar cotizaciones, entre otras. En su mayoría pueden realizarse de manera virtual.
2	Se identifican las tareas críticas y sensibles que podrían requerir medidas adicionales de seguridad para su realización remota, de acuerdo con los principios de gestión de riesgos de ISO/IEC 27002	X		Actualmente cualquier dispositivo con acceso a la red local puede ingresar a cualquier información en el servidor central.	Se debe acatar como primordial la separación de usuarios, roles y privilegios. Así como la creación de políticas que velen por la integridad, disponibilidad y confidencialidad de la información.

No	Aspectos por observar	Cumple	No Cumple	Oportunidad de mejora	Detalle de Observación
3	Se identifican las tareas que no son factibles de realizar de forma remota y se analiza la posibilidad de ajustarlas o mitigar su impacto en la operación, de acuerdo con los requisitos de continuidad del negocio establecidos en ISO/IEC 27001:2022.		X		No se pudo observar a cabalidad la diversidad de tareas durante la visita, ya que las mismas dependen de lo que se tiene planificado para el día.
4	Se examina la infraestructura de red actual para determinar su capacidad para admitir el teletrabajo de manera segura, considerando aspectos como la seguridad de la transmisión de datos y la disponibilidad de conexiones seguras, según lo establecido en ISO/IEC 27001:2022	X		Actualmente cuentan con una infraestructura limitada, sencilla y muy pequeña, sin embargo, se ajusta al tamaño de la empresa actualmente.	Se debe planificar la migración a la nueva infraestructura que se va a proponer ya que inicialmente requerirá de mucho trabajo manual, a causa de la mayor parte de la información estando local y no clasificada apropiadamente.

No	Aspectos por observar	Cumple	No Cumple	Oportunidad de mejora	Detalle de Observación
5	Se evalúa la seguridad de los dispositivos utilizados por los empleados para el trabajo remoto, incluyendo medidas como la autenticación de usuarios y la gestión de parches, siguiendo las directrices de seguridad de la información de ISO/IEC 27002		X	Únicamente para la utilización de correo electrónico se cumple.	Se deben implementar más medidas de seguridad en otros aspectos de la empresa, aparte del correo electrónico para estar en regla con las políticas de los referentes internacionales.
6	Se identifican posibles amenazas y vulnerabilidades asociadas con el teletrabajo, como el acceso no autorizado a datos confidenciales o la pérdida de dispositivos, de acuerdo con los principios de gestión de riesgos de ISO/IEC 27001:2022.	X			No se han identificado ningún tipo de riesgos más allá de los que comúnmente estaríamos expuestos en cualquier ambiente que utilice internet y su exposición inminente a estos riesgos.

Fuente: Elaboración Propia

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA INFORMÁTICA

PROPUESTA INTEGRAL DE OPTIMIZACIÓN Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA: UN ENFOQUE BASADO EN ISO/IEC 27001, ISO/IEC 27002, COBIT, NIST SP 800-46, Y MEJORES PRÁCTICAS DE ITIL

MELANNIE ANGÉLICA MORA CORRALES

JULIO, 2024

CAPÍTULO VI: PROPUESTA

Introducción

CORGIA Gestión e Ingeniería Alternativa es una empresa costarricense ubicada en San José, constituida en el año 2012, con más de una década en el mercado de consultorías eléctricas, son los representantes oficiales a nivel regional (Centroamericano y gran parte de Suramérica) de dos importantes empresas internacionales consultoras eléctricas, fabricantes de herramientas tipo Software para el análisis y simulación de potencia.

Esta se encuentra inscrita al Colegio Federado de Ingenieros y Arquitectos de Costa Rica y su giro de negocio se centra en servicios de consultoría, diseño, simulación e inspección eléctrica, elaboración de estudios de potencia para instalaciones de energía eléctrica, administración y dirección técnica de proyectos eléctricos a nivel industrial, comercial e institucional. De igual manera, brindan el soporte, capacitación y venta de licencias de diseño y análisis de sistemas eléctricos (EasyPower y XGSLab).

La seguridad de la información se ha convertido en un aspecto crítico para las organizaciones, independientemente del tamaño de estas, y especialmente en un entorno donde el acceso remoto y teletrabajo es cada vez más común. La empresa en estudio enfrenta desafíos significativos en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) que se alinee adecuadamente con las normativas ISO/IEC 27001 e ISO/IEC 27002. A continuación, se desarrolla la problemática identificada, basada en un análisis exhaustivo de entrevistas y observaciones dentro de la empresa, destacando las deficiencias en la gestión de la seguridad de la información.

Uno de los problemas más relevantes es la falta de categorización formal de los activos críticos de información, como la información contenida en los respaldos generados, que puede ir desde información innecesaria de años anteriores, hasta información sensible o datos críticos para la continuidad de negocio. Según la normativa ISO/IEC 27001 es esencial comprender el contexto de la organización y las expectativas de las partes interesadas para definir el alcance de la SGSI.

Actualmente la empresa no cuenta con una metodología formal para evaluar y gestionar los riesgos de seguridad de la información.

La empresa carece de políticas y procedimientos formales para la gestión de la seguridad de la información, lo que es un incumplimiento al Capítulo 5 de la norma ISO/IEC 27001. La ausencia de estas políticas representa un factor de riesgo significativo, ya que no se han establecido roles y permisos claros, ni se ha segmentado y restringido adecuadamente el acceso a la información, comprometiendo la confidencialidad, integridad y disponibilidad de datos, fin único de las normas ISO mencionadas.

Aunque se utiliza software antivirus AVG en las computadoras, la empresa no cuenta con un sistema centralizado de gestión de seguridad de la información. La infraestructura actual incluye un servidor de archivos con un sistema operativo obsoleto y un disco duro externo para respaldos, sin políticas formales para la gestión de activos de información. La falta de un sistema centralizado de copias de seguridad puede resultar en la pérdida de datos críticos.

La empresa no proporciona formación regular sobre seguridad de la información a los empleados, lo que aumenta el riesgo de incidentes de seguridad debido a la falta de conciencia y capacitación. Según el Capítulo 7 de la ISO/IEC 27001, es crucial que el personal esté consciente de la política de seguridad y comprenda su contribución al SGSI. De igual manera, no existe un proceso establecido para manejar incidentes de seguridad de la información. La falta de protocolos claros dificulta la respuesta efectiva a amenazas de seguridad. La ISO/IEC 27001 requiere una evaluación de riesgos y una matriz de calificación para categorizar y responder a los eventos de seguridad.

La empresa no realiza auditorías internas periódicas para verificar el cumplimiento de las políticas de seguridad de la información. La falta de revisiones dificulta la identificación de áreas de mejora y el mantenimiento de un nivel adecuado de seguridad. El Capítulo 9 de la ISO/IEC 27001 destaca la importancia de la evaluación del desempeño y las auditorías internas para mantener la eficacia del SGSI.

La problemática identificada en la empresa evidencia una falta de estructuras y procedimientos formales necesarios para cumplir con las normativas ISO/IEC 27001 e ISO/IEC

27002. Es imperativo desarrollar e implementar un SGSI robusto que incluya la identificación y evaluación de riesgos, el establecimiento de políticas y procedimientos claros, la gestión adecuada de accesos, la protección contra malware, la formación del personal, la gestión de incidentes de seguridad y la realización de auditorías internas. Este plan permitirá a la empresa fortalecer su postura de seguridad de la información y garantizar la continuidad del negocio en un entorno cada vez más digital y remoto.

Objetivos

Objetivo General

Diseñar una Propuesta Integral de Optimización y Seguridad de la Infraestructura Tecnológica para la empresa CORGIA Gestión e Ingeniería Alternativa, basada en las normas ISO/IEC 27001, ISO/IEC 27002, COBIT, NIST SP 800-46 y Mejores Prácticas de ITIL, con el propósito de fortalecer la gestión de seguridad de la información y lograr la optimización de los procesos operativos.

Objetivos Específicos

- Desarrollar una propuesta de infraestructura tecnológica que facilite el acceso seguro y remoto a la información, siguiendo los lineamientos de las normas ISO/IEC 27001 y prácticas de ITIL, misma que permita la implementación del teletrabajo de manera efectiva y segura.
- Establecer políticas de seguridad de la información que contemple la creación de roles y separación de permisos dentro de la organización, asegurando que solo los usuarios autorizados tengan acceso a información relevante a sus funciones.
- Crear una configuración uniforme de seguridad en todos los dispositivos utilizados por la empresa, siguiendo las directrices NIST SP 800-53 e ISO/IEC 27001, y desarrollo de estrategia práctica para la realización de copias de seguridad de datos críticos, en concordancia con las normas ISO e ITIL, dichos esfuerzos asegurando la protección de la información y la continuidad operativa de la empresa.

- Crear un manual para la gestión de incidentes de seguridad de la información, estableciendo un plan de auditorías internas y revisión continua del SGSI, siguiendo las directrices ISO/IEC 27001.
- Desarrollar un programa de formación y concienciación en seguridad de la información para todos los empleados, basado en los requisitos de ISO/IEC 27001, para que se asegure que el personal esté adecuadamente capacitado y consciente de las políticas de seguridad.

Alcance Funcional

En esta sección se detalla el alcance funcional de la propuesta para la optimización y seguridad de la infraestructura tecnológica de CORGIA Gestión e Ingeniería Alternativa. Esta propuesta se enmarca en el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) robusto y eficiente, basado en las normas internacionales ISO/IEC 27001, ISO/IEC 27002, y las mejores prácticas de COBIT, NIST SP 800-46, e ITIL. El objetivo principal es fortalecer la gestión de seguridad de la información y optimizar los procesos operativos de la empresa. A continuación, se describen los componentes clave y los entregables que conformarán esta propuesta, asegurando una implementación efectiva y alineada con los estándares mencionados.

Acceso Remoto y Seguro: Diseñar un plan que facilite la migración hacia una infraestructura avanzada que permita el acceso remoto a la información de manera segura, contemplando el uso de una red virtual privada (VPN) como opción principal para asegurar la confidencialidad e integridad de los datos durante las conexiones y transacciones remotas realizadas. Contemplar en este plan, la configuración de medidas de autenticación robustas para garantizar la identidad de los usuarios que acceden de forma remota. Este objetivo se alinea con los lineamientos de las normas ISO/IEC 27001 e ITIL, facilitando un acceso seguro y eficiente a la información, al incluir una guía de prácticas recomendadas que asegure la implementación del teletrabajo de manera efectiva y segura.

Gestión de Seguridad de la Información: Definir y documentar las políticas de seguridad de la información, alineadas con las normas ISO/IEC 27001, ISO/IEC 27002 y COBIT. Políticas en las que se establecerán roles y permisos específicos para cada usuario, garantizando un acceso

controlado y seguro a la información, implementando protocolos que aseguren la disponibilidad de los datos, fortaleciendo la confidencialidad e integridad de la información. Esto implica la creación de un manual de políticas de seguridad que detalle la definición de roles y permisos y una guía para la gestión de accesos y control de usuarios.

Configuración Uniforme de la Seguridad: Establecer estándares de seguridad basados en NIST SP 800-53 e ISO/IEC 27001 para lograr una configuración uniforme en todos los dispositivos. Definir procedimientos y políticas para la instalación de antivirus, configuraciones de cortafuegos y otras medidas esenciales en todos los dispositivos. Garantizar coherencia y robustez en la defensa contra amenazas cibernéticas mediante la aplicación sistemática de los estándares de seguridad definidos. Estos esfuerzos se plasmarán en un conjunto de normativas que aseguren la protección de la información y la continuidad operativa de la empresa.

Gestión de Copias de Seguridad: Desarrollar una guía con estrategias sólidas basadas en las normas ISO e ITIL para la realización periódica y automatizada de copias de seguridad de datos críticos. Contemplando en la guía las debidas recomendaciones para una segmentación eficiente de datos según su importancia y criticidad para la continuidad de negocio, crear procedimientos de prueba para validar la efectividad de los respaldos. Diseñar un plan estratégico que simplifique la aplicación de estas normas en la infraestructura organizacional futura, asegurando que el personal esté capacitado y consciente de las políticas de seguridad.

Gestión de Incidentes y Auditorías Internas: Crear un manual para la gestión de incidentes de seguridad de la información, estableciendo un plan de auditorías internas y revisión continua del Sistema de Gestión de Seguridad de la Información (SGSI), siguiendo las directrices de ISO/IEC 27001. Este manual detallará los procedimientos para la identificación, respuesta y mitigación de incidentes de seguridad, así como la planificación y ejecución de auditorías internas para evaluar la eficacia del SGSI y asegurar su mejora continua.

Programa de Formación y Concienciación: Desarrollar una guía para la creación del programa de formación y concienciación en seguridad de la información para los empleados, basado en los requisitos de ISO/IEC 27001. Este programa garantizará que el personal esté

adecuadamente capacitado y consciente de las políticas de seguridad, contribuyendo a la creación de una cultura de seguridad dentro de la organización.

Este alcance funcional se alinea con los objetivos planteados, asegurando que cada componente del Sistema de Gestión de Seguridad de la Información (SGSI) se aborde de manera integral y estructurada, a través de la creación de documentos, planes y guías que faciliten su implementación y mantenimiento.

Plan de Migración a Infraestructura de Acceso Remoto y Seguro

El documento "Plan de Migración a Infraestructura de Acceso Remoto y Seguro" adjunto como Anexo C, tiene como objetivo guiar a CORGIA Gestión e Ingeniería Alternativa en la transición de su infraestructura de red local (LAN) a una solución que permita el acceso remoto seguro. Se destacan las necesidades de confidencialidad e integridad de los datos, mediante la implementación de una red virtual privada (VPN) y medidas robustas de autenticación, siguiendo normas ISO/IEC 27001 e ITIL.

Para la evaluación de la infraestructura actual, se detalla la infraestructura actual de CORGIA, que incluye un servidor de archivos con Windows 8.1 Pro, una red local con acceso limitado, suscripción a Microsoft Office 365 Family y uso de AVG para la seguridad de 10 dispositivos. Se propone realizar una migración de datos e infraestructura hacia la nube, los objetivos principales son: Facilitar el acceso seguro y remoto a la información, mejorar la colaboración interna y externa, asegurar la confidencialidad, integridad y disponibilidad de los datos y reducir la carga de gestión de infraestructura local.

Como parte de los requisitos de la nueva infraestructura se contempla la implementación de una VPN segura para conexiones remotas, uso de autenticación multifactor (MFA), políticas de contraseñas seguras, cifrado de datos en tránsito y monitoreo de actividades de acceso remoto.

La solución recomendada en la propuesta de migración, se detallan las herramientas a implementar, tales como Office 365 (Microsoft 365 Business Standard), que proporciona herramientas de productividad y colaboración con seguridad avanzada y soporte continuo. WatchGuard UTM, la misma ofrece una solución integral de seguridad que incluye IPsec, cifrado de datos y seguridad web a un costo razonable. Nagios, como el software de monitoreo de red con funcionalidades robustas y escalabilidad, para garantizar el monitoreo de las actividades en WatchGuard y la VPN a utilizar.

Como parte de las etapas de implementación de dicha infraestructura, se detalla en primera instancia la planificación, etapa en la que se realiza una evaluación de recursos, análisis de costos, selección de proveedores y diseño de la arquitectura. Seguidamente, el desarrollo e implementación, etapa en la que se describe el proceso de migración de datos a SharePoint,

configuración de WatchGuard UTM y Nagios, e implementación de MFA. Finalmente, se describen los pasos para la realización de la etapa despliegue y mantenimiento, misma que se siguiere realizar de forma gradual, esta incluye capacitación de empleados a las nuevas herramientas implementadas, monitoreo continuo haciendo uso de los softwares implementados y hacer uso del soporte técnico de cada herramienta contemplado en las subscripciones adquiridas en caso de necesitar apoyo o una guía adicional en la utilización de las mismas.

Se incluye una sección como guía de prácticas recomendadas, misma en la que se sugiere a grandes rasgos, mantener actualizaciones regulares de los softwares implementados, Office 365, WatchGuard UTM y Nagios. Revisar ajustes periódicos de las políticas de seguridad, según las necesidades de nuevos roles, usuarios, sus responsabilidades y accesos, así como la implementación de auditorías regulares en las medidas de seguridad implementadas para asegurar el cumplimiento continuo con las normas ISO/IEC 27001.

El plan propuesto representa un enfoque integral para modernizar la infraestructura tecnológica de CORGIA. Abarca desde la evaluación inicial hasta la implementación y mantenimiento de soluciones avanzadas de acceso remoto seguro. Las soluciones recomendadas, *Office 365*, *WatchGuard UTM* y *Nagios*, ofrecen un equilibrio entre costo y beneficio, compatibilidad con la infraestructura existente y seguridad avanzada. Se destacan las prácticas recomendadas para mantener la seguridad y el rendimiento a lo largo del tiempo, asegurando que la organización esté equipada para enfrentar los desafíos tecnológicos actuales y futuros.

Manual de Gestión de Seguridad de la Información

El "Manual de Gestión de Seguridad de la Información" es una guía completa diseñada para proteger los activos de información de la organización, alineada con las normas ISO/IEC 27001 e ISO/IEC 27002, así como las pautas de COBIT. Su objetivo principal es establecer y documentar políticas de seguridad que aseguren un acceso controlado y seguro a la información, definiendo roles y permisos específicos para cada usuario. La implementación de estas políticas busca garantizar la disponibilidad, confidencialidad e integridad de los datos, mitigando riesgos y cumpliendo con los requisitos legales y regulatorios.

El manual se divide en varias secciones clave, entre estas contamos con las políticas de control de acceso, las mismas establecen directrices para proteger la información contra accesos no autorizados, modificaciones indebidas y pérdida de disponibilidad. Incluyen registro y gestión de usuarios, uso de contraseñas y segmentación de la red.

Seguidamente se contempla la definición de roles y permisos, sección que detalla la identificación de roles dentro de la organización y la asignación de permisos basados en las responsabilidades y necesidades de acceso a la información, para esta se ha especificado un procedimiento guía para la creación de una matriz de control de accesos, ya que esta proporciona una herramienta para garantizar que el acceso a los activos de información esté restringido únicamente a personas autorizadas, implementando controles adecuados para prevenir el acceso no autorizado y asegurar el cumplimiento de las políticas.

Se detalla también, la sección de provisión, revisión y revocación de accesos, esta describe los procedimientos para la solicitud, revisión y revocación de accesos, asegurando que los permisos sean apropiados y que los accesos no utilizados sean eliminados una vez no correspondan a sus responsabilidades. Así como la autenticación y autorización, que implementa mecanismos robustos para verificar la identidad de los usuarios y controlar el acceso a los recursos, como la autenticación multifactorial.

Dentro de las últimas etapas, se contemplan el monitoreo y las auditorías, esta ya que establece procesos para detectar y responder a actividades sospechosas, incluyendo registro de accesos, análisis de registros, implementación de alertas automáticas y auditorías internas y

externas. Sin embargo, de la misma manera se incluyó la capacitación y concienciación, porque proporciona programas de formación regular para todos los empleados sobre las políticas y procedimientos de seguridad, incluyendo concienciación sobre amenazas, capacitación en el uso adecuado de sistemas y simulacros de respuesta a incidentes.

Finalmente, la implementación y mejora continua, sección que detalla la implementación efectiva de las políticas y procedimientos de seguridad y la importancia de la mejora continua a través de evaluaciones periódicas, revisión de roles y permisos, y lecciones aprendidas de incidentes de seguridad y auditorías.

La gestión efectiva de la seguridad de la información es crucial para proteger los activos de información de la organización, garantizando la confidencialidad, integridad y disponibilidad de los datos. Este manual proporciona un manual guía para establecer y mantener políticas y procedimientos de seguridad robustos, capaces de adaptarse a los desafíos emergentes y proteger los activos más valiosos de la organización. La adopción de estas prácticas no solo mitiga riesgos significativos, sino que también fomenta una cultura de seguridad en toda la empresa.

Guía de Configuración Uniforme de Medidas de Seguridad en Dispositivos

Este documento está diseñado para proporcionar a CORGIA Gestión e Ingeniería Alternativa una guía integral para asegurar todos los dispositivos que acceden a su red corporativa. Basado en los estándares internacionales NIST SP 800-53 e ISO/IEC 27001, el manual establece directrices claras y procedimientos específicos para la gestión de la seguridad de los dispositivos. Su objetivo es garantizar que todas las prácticas de seguridad sean consistentes y eficaces en toda la organización, mitigando riesgos y asegurando el cumplimiento normativo.

A través de este documento, se detalla información primordial sobre el inventario de dispositivos: El primer paso crítico es la realización de un inventario completo de todos los dispositivos que acceden a la red corporativa. Este proceso se alinea con el control CM-8 de NIST SP 800-53 y la cláusula A.8.1.1 de ISO/IEC 27001. La guía proporciona métodos y herramientas para identificar, documentar y mantener un registro actualizado de todos los activos tecnológicos importantes.

Seguidamente, se detalla sobre la evaluación de riesgos, el cómo evaluar los riesgos asociados a cada dispositivo mediante el control RA-3 de NIST SP 800-53 y la cláusula A.8.2.1 de ISO/IEC 27001. Incluye directrices para clasificar la información y priorizar las medidas de seguridad basándose en la criticidad y sensibilidad de los datos manejados por cada dispositivo. De la misma manera, se contempla la implementación de medidas de seguridad, tales como antivirus y cortafuegos en todos los dispositivos, siguiendo los controles SI-3 y AC-4 de NIST SP 800-53 y las cláusulas A.12.2.1 y A.13.1.1 de ISO/IEC 27001. También se aborda la configuración de autenticación multifactor (MFA) con Microsoft Authenticator y el cifrado de datos según los controles IA-2 y SC-12 de NIST SP 800-53 y las cláusulas A.9.4.2 y A.10.1.1 de ISO/IEC 27001.

Finalmente, incluye temas relevantes para la seguidad de la información en una compañía, estos siendo las auditorías regulares y capacitación a los empleados de la organización, el documento especifica la necesidad de realizar auditorías de seguridad trimestrales para asegurar el cumplimiento continuo de los estándares, conforme al control CA-7 de NIST SP 800-53 y la cláusula A.18.2.2 de ISO/IEC 27001. Además, se enfatiza la importancia de la capacitación

continua para todos los empleados sobre las mejores prácticas de seguridad, siguiendo el control AT-2 de NIST SP 800-53 y la cláusula A.7.2.2 de ISO/IEC 27001.

La implementación de esta guía permitirá a CORGIA Gestión e Ingeniería Alternativa fortalecer significativamente su postura de seguridad. Al seguir las directrices y procedimientos establecidos, la organización puede asegurar una protección uniforme y robusta de sus dispositivos, reducir los riesgos de seguridad, y cumplir con las normativas internacionales.

Esta guía no solo ayudará a proteger la infraestructura tecnológica de la empresa, sino que también promoverá una cultura de seguridad integral dentro de la organización. Con un compromiso continuo y la actualización regular de las políticas y procedimientos, CORGIA estará mejor preparada para enfrentar los desafíos cibernéticos actuales y futuros, garantizando la sostenibilidad y resiliencia de sus operaciones.

Guía de Gestión de Copias de Seguridad

Esta guía aborda de manera estructurada la gestión de copias de seguridad de información dentro del ámbito empresarial específicamente para CORGIA Gestión e Ingeniería Alternativa, resalta la importancia de mantener la seguridad de la información y la continuidad operativa como pilares fundamentales para el éxito y la resiliencia de la organización.

En la introducción, se pone de manifiesto la necesidad de implementar estrategias para realizar copias de seguridad periódicas y automatizadas de datos críticos, siguiendo normas internacionales como ISO/IEC 27001, ISO/IEC 27002 e ITIL. El manual subraya la importancia de segmentar los datos según su criticidad y diseñar procedimientos de prueba para validar la efectividad de los respaldos. Además, se plantea la implementación de una infraestructura tecnológica avanzada y segura que optimice los procesos operativos y fortalezca la seguridad de la información.

Los objetivos de la guía se centran en establecer estándares consistentes para la realización de copias de seguridad en todos los sistemas críticos, definir procedimientos y políticas claras, garantizar la integridad y disponibilidad de las copias de seguridad mediante pruebas periódicas, promover la continuidad operativa y capacitar al personal para asegurar que estén conscientes de las políticas de seguridad y respaldo.

La implementación de esta guía se espera que aporte numerosos beneficios, como la protección de datos críticos, la disponibilidad y recuperación rápida de la información, el cumplimiento normativo, la optimización de recursos, una mayor confianza del cliente y una mejora en la postura de seguridad de la organización. El manual también describe las políticas y controles necesarios, basándose en normas internacionales anteriormente mencionadas, para la clasificación y manejo de la información. Además, menciona las mejores prácticas de ITIL para la gestión de servicios de TI, enfatizando la importancia de una estrategia sólida de respaldo y recuperación de datos.

Los procedimientos específicos detallados en la guía incluyen la identificación y clasificación de datos según su criticidad y sensibilidad, la definición de la frecuencia y programación de los respaldos, la realización de pruebas regulares para asegurar la restauración

efectiva de la información respaldada, y la garantía de la protección física y ambiental de las copias de seguridad.

En conclusión, el manual proporciona a CORGIA una hoja de ruta clara para mejorar la gestión de copias de seguridad, asegurando la protección y disponibilidad de datos críticos y fortaleciendo su posición competitiva en el mercado. Este documento ofrece un marco completo para la gestión de copias de seguridad, alineado con estándares internacionales y mejores prácticas, con el objetivo de asegurar la continuidad operativa y la seguridad de la información dentro de la organización.

Manual de Gestión de Incidentes y Auditorías Internas

El manual de gestión de incidentes y auditorías internas de CORGIA, basado en la norma ISO/IEC 27001 e ISO/IEC 27002, constituye un recurso integral para asegurar la protección efectiva y la gestión adecuada de la seguridad de la información dentro de la organización. Su objetivo principal es establecer procedimientos sistemáticos para manejar incidentes de seguridad, así como para planificar y ejecutar auditorías internas de manera efectiva.

En su introducción, el manual describe su alcance, aplicándose a todos los sistemas y procesos de CORGIA que manejan información crítica y sensible. Esto incluye desde estaciones de trabajo y servidores hasta dispositivos móviles, asegurando una cobertura completa para la protección de los activos de información.

La gestión de incidentes de seguridad se aborda, comenzando por la definición y establecimiento de canales claros para la detección y reporte de incidentes. Se describen los pasos para la evaluación inicial, clasificación según la severidad y el impacto, y la asignación de recursos adecuados para la respuesta y mitigación rápida de los incidentes. Además, se enfatiza la importancia de medidas como la contención inmediata, la erradicación de la causa raíz y la recuperación de los sistemas afectados, seguidas de un análisis post-incidente para aprender de las experiencias y actualizar las políticas de seguridad correspondientes.

Las auditorías internas son otro componente crucial del manual, programadas regularmente para evaluar la efectividad del Sistema de Gestión de Seguridad de la Información (SGSI). Se define claramente el alcance de cada auditoría y se designa un equipo competente e independiente para llevar a cabo las revisiones. Durante las auditorías, se recopila información relevante a través de entrevistas, observaciones y evaluaciones técnicas, culminando en la elaboración de informes detallados que se revisan con el equipo de seguridad. A partir de los hallazgos, se desarrollan planes de acción para implementar correcciones y mejoras necesarias.

La mejora continua es un principio rector del manual, enfocándose en la revisión constante y la actualización de procesos y controles de seguridad para mantener la eficacia del SGSI. Además, se subraya la importancia del cumplimiento con los requisitos normativos y estándares

internacionales, asegurando la recolección rigurosa de evidencias que respalden la conformidad durante auditorías externas.

Finalmente, se implementa en el siguiente manual, un programa de capacitación y concienciación para el personal de CORGIA, garantizando que todos comprendan y cumplan con las políticas de seguridad establecidas. En conjunto, este manual no solo fortalece la capacidad de CORGIA para enfrentar y mitigar riesgos de seguridad, sino que también refuerza su compromiso con la protección de la información crítica y la confianza de sus clientes y socios comerciales.

Programa de Formación y Concienciación en Seguridad de la Información

Este manual ofrece una guía detallada para la creación de un Programa de Formación y Concienciación en Seguridad de la Información, basado en los requisitos de la norma ISO/IEC 27001. El objetivo principal es garantizar que todos los empleados de la organización estén adecuadamente capacitados y conscientes de las políticas de seguridad, fomentando una cultura de seguridad robusta. El programa abarca todos los niveles de personal, desde la alta dirección hasta los empleados operativos, e incluye varias áreas clave. Primero, cubre las políticas y procedimientos de seguridad, describiendo en detalle las políticas de la organización, los procedimientos para la gestión de datos sensibles y la protección de la infraestructura de TI, y las responsabilidades de cada empleado.

En cuanto a la formación técnica y operativa, el programa proporciona capacitación en el uso seguro de herramientas y sistemas informáticos, métodos de autenticación, gestión de contraseñas, y el manejo seguro de dispositivos móviles y el acceso remoto. Además, se centra en la concienciación sobre amenazas y vulnerabilidades, ofreciendo información sobre amenazas comunes como el phishing, malware y ataques de ingeniería social, y estrategias para mitigar estas vulnerabilidades.

Para la respuesta a incidentes de seguridad, el programa establece procedimientos claros para reportar y gestionar incidentes, incluyendo simulacros y ejercicios prácticos para preparar a los empleados en la respuesta efectiva a incidentes. La evaluación y certificación continua del conocimiento y la comprensión de los empleados sobre las políticas de seguridad asegura que cumplan con los estándares establecidos. La actualización y mejora continua es otro componente esencial del programa. Se realiza una revisión semestral y una actualización anual del contenido de formación para incluir nuevas amenazas, tecnologías y mejores prácticas.

La implementación de este programa es crucial para proteger los activos de información y fomentar una cultura de seguridad dentro de la organización. A través de la capacitación continua y la actualización del contenido, se garantiza que los empleados estén preparados para enfrentar amenazas emergentes y aplicar las mejores prácticas en seguridad de la información.

APÉNDICE A

Plan de Migración a Infraestructura de Acceso Remoto y Seguro.

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA INFORMÁTICA

PLAN DE MIGRACIÓN A INFRAESTRUCTURA DE ACCESO REMOTO Y SEGURO

MELANNIE ANGÉLICA MORA CORRALES

JULIO, 2024

CONTENIDOS

INTRODUCCIÓN

Este plan tiene como objetivo facilitar la migración de CORGIA Gestión e Ingeniería Alternativa desde su infraestructura de red local (LAN) actual a una solución que permita el acceso remoto seguro a la información. Este proceso incluirá la implementación de una red virtual privada (VPN) como opción principal para asegurar la confidencialidad e integridad de los datos durante las conexiones remotas. Además, se contemplarán medidas de autenticación robustas para garantizar la identidad de los usuarios que acceden de forma remota, alineándose con los lineamientos de las normas ISO/IEC 27001 e ITIL.

Evaluación de la Infraestructura Actual

Antes de iniciar la migración, es crucial entender la infraestructura actual de CORGIA Gestión e Ingeniería Alternativa. Actualmente, la empresa opera con la siguiente configuración:

- Servidor de archivos: Sistema operativo Windows 8.1 Pro con carpetas compartidas accesibles a través de la red local.
- Red local (LAN): Dispositivos conectados a través de una red local con acceso limitado fuera de las instalaciones de la empresa.
- Carpeta compartida accesible a través de la red local.
- Seguridad: Uso de AVG para 10 dispositivos con suscripción por 2 años, que incluye: AVG Internet Security, AVG TuneUp, AVG Secure VPN, AVG AntiTrack.
- Almacenamiento en la nube: Suscripción de Microsoft Office 365 Family, que proporciona acceso a OneDrive con 1TB por usuario para hasta 5 usuarios.

ITIL 5.2.6 (Gestión de Activos de TI): *Gestión y control de los activos de TI utilizados por la organización, asegurando que estén registrados, actualizados y gestionados adecuadamente.*

Objetivos de la Migración a la Nube

- Acceso Remoto: Facilitar el acceso seguro y remoto a la información y aplicaciones desde cualquier ubicación y dispositivo.

ITIL 5.2.12 (Gestión de la Continuidad del Servicio): *Asegurar que los servicios críticos de TI estén disponibles para soportar los procesos de negocio.*

- Colaboración: Mejorar la colaboración interna y externa mediante herramientas de comunicación y colaboración en tiempo real.

ITIL 4.2 (Gestión de la Demanda): *Entender y gestionar la demanda de servicios de TI, facilitando la colaboración interna y externa mediante herramientas de comunicación en tiempo real.*

- Seguridad: Asegurar la confidencialidad, integridad y disponibilidad de los datos con medidas de seguridad avanzadas y autenticación robusta.

ITIL 5.1.3 (Gestión de Seguridad de la Información): *Proteger la información y los sistemas de TI contra riesgos mediante medidas de seguridad avanzadas y autenticación robusta.*

- Eficiencia Operativa: Reducir la carga de gestión de infraestructura local, permitiendo que el equipo de TI se concentre en actividades estratégicas.

ITIL 5.2 (Gestión de Servicios de TI): *Optimizar la gestión de la infraestructura y liberar recursos para actividades estratégicas.*

Requisitos de la Nueva Infraestructura

Red Virtual Privada (VPN)

- Implementación de una VPN para asegurar las conexiones remotas.
- Selección de un protocolo de VPN seguro.
- Configuración VPN en la infraestructura existente.

ITIL 3.2 (Gestión de Redes y Conectividad): *Gestionar y optimizar las redes y la conectividad de TI, incluyendo la implementación de VPN para asegurar las conexiones remotas.*

Medidas de Autenticación Robustas

- Implementación de autenticación multifactorial (MFA).
- Políticas de contraseñas seguras y su renovación periódica.

ITIL 5.1.3 (Gestión de Seguridad de la Información): *Implementación de autenticación multifactor (MFA) y políticas de contraseñas seguras para proteger los sistemas de TI.*

Seguridad Adicional

- Cifrado de datos en tránsito.
- Monitoreo y registro de actividades de acceso remoto.
- Capacitar a los empleados sobre buenas prácticas de seguridad y uso de la nueva infraestructura.

ITIL 5.1.3 (Gestión de Seguridad de la Información): *Protección de la información contra riesgos, asegurando la confidencialidad, integridad y disponibilidad de los datos.*

ITIL 5.1.3 (Gestión de Seguridad de la Información): *Cifrado de datos en tránsito, monitoreo y registro de actividades de acceso remoto, y capacitación en buenas prácticas de seguridad.*

SOLUCIÓN RECOMENDADA

Office 365 (Microsoft 365 Business Standard)

Equilibrio entre Costo y Beneficio

Office 365 Business Standard, con un costo de $12.50 por usuario al mes, este plan ofrece un conjunto completo de herramientas de productividad y colaboración que incluye aplicaciones de Office, correo electrónico, OneDrive (1 TB), Teams y SharePoint. Esta solución proporciona una excelente relación costo-beneficio, ya que permite una migración completa a la nube, optimizando la gestión de documentos y la colaboración en equipo, así como mínima inversión en equipo físico y costos de mantenimiento y administración reducidos.

Compatibilidad con Infraestructura Existente

Office 365 es altamente compatible con la infraestructura tecnológica existente de CORGIA, de hecho, cuentan con un plan Microsoft y sus cuentas personales actualmente, permitiendo una integración sin problemas. La solución se puede implementar sin necesidad de cambios radicales, reduciendo el tiempo de implementación y los costos asociados con la transición.

Facilidad de Implementación

Office 365 es conocido por su facilidad de instalación y configuración. Las herramientas integradas de migración y administración facilitan el proceso de mover datos y usuarios a la nube, lo que es ideal para una empresa que busca adoptar tecnologías de acceso remoto seguro y colaboración en línea.

Seguridad y Fiabilidad

Seguridad Avanzada: Office 365 proporciona seguridad de nivel empresarial, incluyendo características como autenticación multifactor (MFA), protección contra amenazas avanzadas, y cifrado de datos en tránsito y en reposo. Estas características son esenciales para proteger los datos y garantizar la integridad y confidencialidad durante las conexiones remotas.

Autenticación Robusta: Office 365 soporta autenticación multifactor (MFA), asegurando que solo los usuarios autorizados puedan acceder a la red y a los recursos de la empresa, alineándose con las mejores prácticas de seguridad recomendadas por ISO/IEC 27001 e ITIL.

ITIL 5.2 (Gestión de Servicios de TI): *Proveer herramientas de productividad y colaboración, seguridad avanzada, soporte técnico continuo y actualizaciones regulares.*

Soporte y Actualizaciones

Microsoft ofrece soporte técnico continuo y actualizaciones regulares de software, asegurando que la solución esté siempre protegida contra las últimas amenazas y cumpla con los estándares de seguridad más recientes. Esto incluye mejoras de funcionalidad y parches de seguridad que son cruciales para mantener la integridad del sistema.

Recomendación de Solución VPN y Seguridad: WatchGuard UTM

- Equilibrio entre Costo y Beneficio: WatchGuard UTM con un costo anual de $365, ofrece una solución de seguridad integral que incluye IPsec, encriptación, seguridad web, antivirus y control de aplicaciones. Este precio es competitivo y proporciona una amplia gama de funcionalidades de seguridad a un costo razonable.
- Integración y Compatibilidad: WatchGuard UTM es compatible con la infraestructura tecnológica existente y se integra sin necesidad de cambios drásticos, facilitando la migración y asegurando una implementación eficiente.
- Seguridad Avanzada: WatchGuard UTM proporciona seguridad de nivel empresarial con características avanzadas como IPsec, encriptación y seguridad web, garantizando la protección de los datos durante las conexiones remotas y las transacciones.
- Actualizaciones Regulares y Soporte: WatchGuard ofrece soporte técnico continuo y actualizaciones regulares, asegurando que la solución esté siempre protegida contra las últimas amenazas y cumpla con los estándares de seguridad más recientes.

ITIL 3.2 (Gestión de Redes y Conectividad): *Proveer seguridad de nivel empresarial con características avanzadas de encriptación y monitoreo de redes.*

Software de Monitoreo Recomendado: Nagios

- Funcionalidad Integral: Nagios proporciona herramientas robustas de monitoreo de red, incluyendo monitoreo de tráfico, análisis de ancho de banda, monitoreo de servidores y aplicaciones, y alertas en tiempo real. Permite una vigilancia proactiva y la identificación temprana de posibles problemas.
- Costo: Nagios ofrece una versión gratuita con funcionalidades básicas y opciones de pago para características avanzadas. Esta flexibilidad permite a las empresas adaptar la solución a sus necesidades y presupuesto.
- Interfaz Intuitiva: Nagios es conocido por su facilidad de uso y configuración, facilitando la adopción de la herramienta sin necesidad de una capacitación extensa.
- Nagios es altamente escalable, permitiendo a la empresa añadir más capacidades de monitoreo a medida que su red y necesidades crecen.

ITIL 5.2.7 (Gestión de Monitoreo y Eventos): *Proveer herramientas robustas de monitoreo de red, incluyendo análisis de tráfico, monitoreo de servidores y alertas en tiempo real.*

Seguridad Adicional y Medidas de Autenticación

Implementación de Autenticación Multifactor (MFA)

- Software Recomendado: Los usuarios pueden utilizar la aplicación Microsoft Authenticator para recibir notificaciones push en sus dispositivos móviles y aprobar o denegar el inicio de sesión con un toque. También puede generar códigos de verificación sin conexión.
- Métodos de Autenticación: Aplicaciones de autenticación, los usuarios pueden optar por recibir un código de verificación a través de un mensaje de texto en su teléfono móvil, una llamada telefónica entre otros.

Políticas de Contraseñas Seguras

- Requisitos: Longitud mínima, complejidad (mezcla de caracteres), renovación periódica.
- Gestión de Contraseñas: Uso de gestores de contraseñas (e.g., LastPass, 1Password).

ETAPAS DE IMPLEMENTACIÓN

Planificación

1. **Evaluación de Recursos**

   Cómo: Identificar los recursos necesarios (hardware, software, personal técnico) para implementar Office 365, WatchGuard UTM y Nagios. Establecer un inventario de activos y evaluar la compatibilidad de hardware existente.

ISO/IEC 27001 (A.8.1): *Mantener un inventario actualizado de activos de información. EL objetivo de este punto es la identificación de los activos de información y las responsabilidades sobre los mismos, con el objetivo de evaluar las medidas de protección adecuadas para cada activo en base a una evaluación de riesgos*

ITIL 5.2.6 (Gestión de Activos y Configuración de TI): *Identificar y gestionar los activos necesarios para la implementación.*

2. **Análisis de Costos y Presupuesto**

   Cómo: Realizar un análisis detallado de costos para la adquisición de licencias, hardware y servicios profesionales. Definir un presupuesto y obtener aprobación.

Software	Costo	Frecuencia de Pago
Office 365	$12.50 por usuario	Mensual
WatchGuard UTM	$1400 instalación inicial	Única vez
WatchGuard Licencia	$365	Anual
AGV Security	$60	Anual
Nagios	NA	NA

Fuente: Elaboración Propia

ITIL 5.1.11(Gestión Financiera): *Definir y gestionar los costos y el presupuesto para la implementación.*

3. **Selección de Proveedores:**

Cómo: Evaluar y seleccionar proveedores para Office 365, WatchGuard UTM y Nagios. Realizar una comparación de ofertas y seleccionar los mejores proveedores.

- Microsoft Office proveedor oficial O365.
- Tecnova Soluciones configuración WatchGuard y administración de reglas de seguridad.

ISO/IEC 27001 (A.15.1): *Asegurar la seguridad en las relaciones con proveedores. La relación con un proveedor normalmente está regulada por un contrato de prestación de servicios, es aquí donde se debe reflejar las condiciones para el manejo adecuado de la información de nuestra organización de acuerdo con los requisitos de seguridad que hayamos definido.*

ITIL 2.2.1 (Gestión de Proveedores): *Evaluar y seleccionar proveedores adecuados para los servicios y productos necesarios.*

4. Diseño de la Arquitectura:

Cómo:

a. Migración de Datos: Definir la arquitectura (estructura de la carpeta) para la migración de datos de la carpeta compartida local a SharePoint.
b. Configuración de Permisos: Planificar la configuración de carpetas y la asignación de permisos en SharePoint según roles de usuarios.
c. Integración de VPN y Monitoreo: Diseñar la integración de VPN y Nagios con Office 365 y WatchGuard T20.
d. Políticas de Seguridad y MFA: Establecer políticas de seguridad y configuraciones de MFA.

ISO/IEC 27001 (A.9.1): *Control de acceso a la información, esta política detalla los requisitos para definir las reglas de control de acceso a la información, es decir, los derechos y restricciones de acceso a la información.*

ITIL 5.2.13 (Diseño del Servicio): *Diseñar la arquitectura de la solución, incluyendo la migración de datos y la configuración de permisos y seguridad.*

El principio básico para la elaboración de estas reglas es:

- La asignación de la menor cantidad de privilegios posibles para llevar a cabo una tarea dentro de un sistema de información.
- La concesión de esos privilegios solamente por el tiempo que sea necesario para el desarrollo de las tareas.

Desarrollo e Implementación

Migración de Datos a SharePoint:

1. Crear carpetas y organizar la información en SharePoint de acuerdo con la estructura deseada de la carpeta compartida local. Para crear dichas carpetas y organizar la información siga los siguientes pasos:
    1. Abra la biblioteca de documentos:
        i. Diríjase al sitio de SharePoint donde se encuentra la biblioteca de documentos que quieres usar.
        ii. Haga clic en el nombre de la biblioteca de documentos en la navegación del sitio.
    2. Crear una nueva carpeta:
        i. En la barra de herramientas de la biblioteca de documentos, haga clic en el botón "Nuevo".
        ii. En el menú desplegable, seleccione "Carpeta".
    3. Nombre de la carpeta:
        i. Aparecerá un cuadro de diálogo que pedirá que introduzcas un nombre para la nueva carpeta.
        ii. Escriba el nombre que deseas darle a la carpeta.
        iii. Después de escribir el nombre, haga clic en el botón "Crear" o presione Enter.
    4. Ver la nueva carpeta:
        i. La nueva carpeta aparecerá en la lista de documentos de la biblioteca.
        ii. Puede hacer clic en el nombre de la carpeta para abrirla y empezar a agregar documentos en ella.

Estos pasos le permitirán organizar mejor sus documentos en SharePoint creando carpetas dentro de tus bibliotecas de documentos. Sírvase de utilizar la siguiente documentación guía oficial de Microsoft Crear una carpeta en una biblioteca de documentos. (Microsoft Corporation, 2024)

2. Establecer roles y permisos de acceso en SharePoint para los usuarios según sus funciones y responsabilidades. Para su realización, siga los siguientes pasos que detallo a continuación:
    1. Ir a la configuración del sitio:
        i. Abra su sitio de SharePoint.
        ii. Haga clic en el ícono de engranaje (Configuración) en la esquina superior derecha.
        iii. Seleccione "Configuración del sitio".
    2. Acceder a permisos del sitio:
        i. En la página de Configuración del sitio, en la sección "Usuarios y permisos", haga clic en "Permisos del sitio".
    3. Ver los permisos actuales:
        i. En la página de Permisos del sitio, podrá ver los grupos y usuarios con sus respectivos niveles de permisos.
    4. Modificar permisos de un usuario o grupo:
        i. Seleccione el usuario o grupo cuyo permiso desea modificar haciendo clic en la casilla junto a su nombre.
        ii. Haga clic en "Editar permisos".
        iii. Elija el nuevo nivel de permisos que desea asignar (por ejemplo, "Lectura", "Colaboración", "Control total").
        iv. Haga clic en "Aceptar".
    5. Agregar un nuevo usuario o grupo:
        i. En la página de Permisos del sitio, haga clic en "Conceder permisos".
        ii. En el cuadro de diálogo, escriba el nombre o dirección de correo electrónico del usuario o grupo que desea agregar.
        iii. Seleccione el nivel de permisos que desea asignar.

iv. Haga clic en "Compartir".

6. Eliminar permisos de un usuario o grupo:
    i. Seleccione el usuario o grupo cuyos permisos desea eliminar haciendo clic en la casilla junto a su nombre.
    ii. Haga clic en "Eliminar permisos del usuario".
    iii. Confirme que desea eliminar los permisos.
7. Crear un nuevo nivel de permisos:
    i. En la página de Permisos del sitio, haga clic en "Configuración de permisos".
    ii. Haga clic en "Agregar un nivel de permisos".
    iii. Escriba un nombre y descripción para el nuevo nivel de permisos.
    iv. Seleccione las acciones que este nivel de permisos permitirá.
    v. Haga clic en "Crear".

Estos pasos le ayudarán a gestionar de manera efectiva los permisos de usuario y los niveles de permisos en su sitio de SharePoint, asegurando que todos los usuarios tengan el acceso adecuado según sus necesidades. Sírvase de revisar a más detalle la guía oficial del proveedor en caso de dudas. Permisos y niveles de permisos de usuario en SharePoint Online. (Microsoft Corporation, 2023)

3. Compartir las carpetas relevantes con los usuarios adecuados.

ISO/IEC 27001 (A.12.3): *Protección contra amenazas de software malintencionado. Esta política trata de evitar pérdidas de disponibilidad o rendimiento de los sistemas por falta de capacidad.*

ITIL 4.5.4 (Gestión de la Transición del Servicio): *Gestionar la migración de datos y la configuración de la nueva infraestructura.*

Configuración de WatchGuard UTM:

Cómo:

1. Instalar y configurar el dispositivo para seguridad perimetral. Para instalar y configurar el WatchGuard UTM, se sugiere seguir los siguientes pasos que se detallan a continuación:

a. Descargar el instalador:
    i. Abra su navegador web y vaya al sitio de WatchGuard.
    ii. Inicie sesión con su cuenta de WatchGuard.
    iii. Navegue hasta la sección de descargas y localice el instalador del software cliente de WatchGuard.
b. Ejecutar el instalador:
    i. Una vez descargado, localice el archivo del instalador en su carpeta de descargas.
    ii. Haga doble clic en el archivo del instalador para ejecutarlo.
c. Seguir las instrucciones del asistente de instalación:
    i. Aparecerá una ventana del asistente de instalación.
    ii. Haga clic en "Siguiente" para continuar con el proceso de instalación.
d. Aceptar los términos de la licencia:
    i. Lea los términos del acuerdo de licencia.
    ii. Si está de acuerdo, seleccione la opción "Acepto los términos del acuerdo de licencia".
    iii. Haga clic en "Siguiente".
e. Elegir la ubicación de instalación:
    i. Seleccione la carpeta donde desea instalar el software.
    ii. Haga clic en "Siguiente".
f. Configurar las opciones de instalación:
    i. Puede seleccionar las opciones adicionales que desee instalar.
    ii. Haga clic en "Siguiente".
g. Instalar el software:
    i. Haga clic en "Instalar" para comenzar la instalación.
    ii. Espere a que el proceso de instalación se complete.
h. Finalizar la instalación:
    i. Una vez finalizada la instalación, haga clic en "Finalizar".
    ii. Es posible que se le pida reiniciar su computadora para completar la instalación.

i. Verificar la instalación:
    i. Después de reiniciar, abra el software cliente de WatchGuard para asegurarse de que se haya instalado correctamente.
    ii. Inicie sesión con sus credenciales de WatchGuard.

Estos pasos le guiarán a través de la instalación del software cliente de WatchGuard UTM, asegurando una configuración adecuada y segura en su sistema. De la misma manera se adjunta la guía oficial proporcionada por WatchGuard. La guía detalla los pasos necesarios para la instalación, configuración de seguridad perimetral, reglas de firewall, y establecimiento de conexiones VPN. Instalar el Software Cliente de WatchGuard. (WatchGuard, 2023)

2. Reglas de Firewall: Configurar reglas de firewall para permitir el acceso seguro a Office 365 y otras herramientas internas que permitan la realización de las labores, las mismas se encuentran en una guía proporcionada por el proveedor WatchGuard Acerca de las Reglas y Conjuntos de Reglas. (WatchGuard, 2018)
    a. Abrir la interfaz de administración de Fireware:
        i. Inicie sesión en la interfaz de administración de WatchGuard Fireware usando su navegador web.
    b. Acceder a la sección de Proxies:
        i. En el menú principal, haga clic en "Política" o "Policy" (según el idioma de su interfaz).
        ii. Luego, seleccione "Proxies" para acceder a la configuración de proxies.
    c. Seleccionar el conjunto de reglas:
        i. En la sección de Proxies, encontrará una lista de los conjuntos de reglas configurados.
        ii. Elija el conjunto de reglas que desea configurar o modifique.
    d. Configurar un conjunto de reglas:
        i. Haga clic en el nombre del conjunto de reglas que desea editar.
        ii. Se abrirá una ventana o una nueva página con opciones para modificar el conjunto de reglas.
    e. Agregar, cambiar o eliminar reglas:

i. Para agregar una nueva regla, haga clic en el botón "Agregar" o "Add". Ingrese los detalles de la nueva regla y guarde los cambios.
ii. Para cambiar una regla existente, seleccione la regla que desea modificar y haga clic en "Editar" o "Edit". Realice los cambios necesarios y guarde los ajustes.
iii. Para eliminar una regla, seleccione la regla que desea eliminar y haga clic en "Eliminar" o "Delete". Confirme la eliminación si se le solicita.

f. Aplicar y guardar los cambios:
    i. Una vez que haya terminado de agregar, cambiar o eliminar reglas, asegúrese de guardar los cambios.
    ii. Haga clic en "Guardar" o "Apply" para aplicar las modificaciones al conjunto de reglas.
g. Verificar la configuración:
    i. Revise la lista de reglas para asegurarse de que los cambios se hayan aplicado correctamente.
    ii. Realice pruebas para confirmar que las nuevas reglas están funcionando según lo esperado.

Estos pasos le permitirán configurar y gestionar los conjuntos de reglas en WatchGuard Fireware, asegurando que su configuración de proxy esté ajustada a sus necesidades.

3. Finalmente establecer reglas de VPN para la conexión remota. Configurar VPN Administradas. (WatchGuard, 2023)
    a. Abrir la interfaz de administración de Fireware:
        i. Inicie sesión en la interfaz de administración de WatchGuard Fireware usando su navegador web.
    b. Acceder a la sección de VPN:
        i. En el menú principal, haga clic en "VPN" para acceder a la configuración de VPNs.
    c. Seleccionar la opción de VPN gestionada:

i. En la sección de VPN, busque y seleccione la opción para configurar "VPN gestionadas" o "Managed VPNs".

d. Agregar una nueva VPN gestionada:
    i. Haga clic en el botón "Agregar" o "Add" para crear una nueva VPN gestionada.
    ii. Complete los detalles necesarios para la nueva VPN, como el nombre, la dirección IP del servidor y la configuración de seguridad.
e. Configurar parámetros de la VPN:
    i. Introduzca la configuración de los parámetros de la VPN, como el protocolo de encriptación, los ajustes de autenticación y cualquier otra opción específica que requiera la VPN.
f. Asignar políticas de acceso:
    i. Defina las políticas de acceso para la VPN gestionada. Esto incluye especificar qué recursos estarán disponibles a través de la VPN y establecer las reglas de tráfico permitidas.
g. Guardar y aplicar la configuración:
    i. Haga clic en "Guardar" o "Apply" para guardar la configuración de la VPN gestionada.
    ii. Asegúrese de que la nueva VPN esté activa y correctamente configurada en la lista de VPNs gestionadas.
h. Verificar la conexión de la VPN:
    i. Compruebe que la VPN gestionada se haya establecido correctamente realizando una prueba de conexión.
    ii. Asegúrese de que los dispositivos puedan conectarse a la VPN y acceder a los recursos permitidos.

Estos pasos le permitirán configurar y gestionar VPNs en WatchGuard Fireware, asegurando que su red esté protegida y accesible según sus necesidades.

Integración de Nagios:

Cómo:

1. Instalar y configurar Nagios para monitorear la infraestructura de TI, incluidos los servicios de Office 365 y la conectividad VPN. El mismo se puede realizar siguiendo la documentación oficial Quickstart Installation Guides. (Nagios, s.f.)
    a. Preparar el sistema:
        i. Asegúrese de que su sistema operativo esté actualizado.
        ii. Instale las dependencias necesarias usando el siguiente comando:

```
sudo apt-get update
sudo apt-get install -y build-essential libgd-dev libapache2-mod-
php php php-gd
```

    b. Crear un usuario y grupo para Nagios:
        i. Cree un usuario y grupo para Nagios usando estos comandos:

```
sudo useradd nagios
sudo useradd nagios
sudo usermod -a -G nagios www-data
```

    c. Descargar Nagios Core:
        i. Vaya a la página de descargas de Nagios y copie el enlace del archivo tar.gz.
        ii. Descargue el archivo usando wget. Reemplace <url_del_archivo> con el enlace copiado:

```
wget <url_del_archivo>
```

    d. Descomprimir y compilar Nagios Core:
        i. Descomprima el archivo descargado:

```
tar xzf nagios-*.tar.gz
```

        ii. Acceda al directorio descomprimido:

```
cd nagios-*
```

        iii. Compile e instale Nagios Core:

```
sudo ./configure --with-httpd-conf=/etc/apache2/sites-enabled
sudo make all
sudo make install
sudo make install-init
sudo make install-config
```

```
sudo make install-commandmode
sudo make install-webconf
```

e. Configurar el acceso web:
    i. Configure una contraseña para el usuario web de Nagios:

```
sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

    ii. Ingrese una contraseña cuando se le solicite.

f. Iniciar Nagios Core:
    i. Habilite el servicio de Nagios para que inicie automáticamente:

```
sudo systemctl enable nagios
sudo systemctl start nagios
```

g. Reiniciar Apache:
    i. Reinicie el servidor web Apache para aplicar la configuración:

```
sudo systemctl restart apache2
```

h. Acceder a la interfaz web:
    i. Abra su navegador web y diríjase a http://<ip_del_servidor>/nagios.
    ii. Inicie sesión con el nombre de usuario nagiosadmin y la contraseña que configuró.

i. Configurar los hosts y servicios:
    i. Edite el archivo de configuración de Nagios para agregar nuevos hosts y servicios:

```
sudo nano /usr/local/nagios/etc/objects/localhost.cfg
```

    ii. Añada las definiciones de hosts y servicios según sus necesidades.

j. Verificar la configuración:
    i. Verifique que la configuración de Nagios sea correcta:

```
sudo nagios -v /usr/local/nagios/etc/nagios.cfg
```

    ii. Asegúrese de que no haya errores en la configuración.

k. Reiniciar Nagios Core:
    i. Después de realizar cambios en la configuración, reinicie el servicio de Nagios para aplicar las modificaciones:

```
sudo systemctl restart nagios
```

l. Monitorear y ajustar:
    i. Monitoree su sistema a través de la interfaz web de Nagios.
    ii. Realice ajustes y configuraciones adicionales según sea necesario.

Estos pasos le ayudarán a instalar y configurar Nagios Core para que pueda comenzar a monitorear su infraestructura de TI.

2. Configurar alertas y notificaciones para detectar y responder a posibles problemas de manera proactiva. Nagios Core Notifications. (Nagios, s.f.)

Implementación de MFA

Seleccionar e implementar una solución de MFA con Microsoft Authenticator, siguiendo el paso a paso que detallo a continuación:

1. Descargar Microsoft Authenticator:
    a. Vaya a la tienda de aplicaciones de su dispositivo móvil (App Store para iOS o Google Play Store para Android).
    b. Busque "Microsoft Authenticator" y descárguelo.
    c. Instale la aplicación en su dispositivo móvil.
2. Iniciar sesión en Microsoft 365:
    a. Abra su navegador web y vaya a Microsoft 365.
    b. Inicie sesión con su cuenta de Microsoft 365.
3. Acceder a la configuración de seguridad:
    a. Haga clic en su foto de perfil en la esquina superior derecha.
    b. Seleccione "Ver cuenta" o "Account".
4. Configurar verificación en dos pasos:
    a. En el panel de navegación, haga clic en "Seguridad" o "Security".
    b. Seleccione "Métodos de verificación" o "Sign-in options".
5. Agregar un método de autenticación:
    a. Haga clic en "Agregar método" o "Add method".
    b. En el menú desplegable, seleccione "Aplicación de autenticación" o "Authenticator app".
    c. Haga clic en "Agregar" o "Add".

6. Configurar la aplicación Authenticator:
    a. Abra la aplicación Microsoft Authenticator en su dispositivo móvil.
    b. Toque el símbolo de "+" para agregar una nueva cuenta.
    c. Seleccione "Cuenta personal" o "Cuenta de trabajo o escuela".
    d. Si se le pide, escanee el código QR que aparece en su pantalla de Microsoft 365 usando la aplicación Authenticator.
7. Confirmar la configuración:
    a. Después de escanear el código QR, la aplicación Authenticator generará un código de verificación.
    b. Ingrese el código de verificación en el sitio de Microsoft 365 para completar la configuración.
8. Guardar y confirmar:
    a. Una vez ingresado el código, haga clic en "Verificar" o "Verify" en Microsoft 365.
    b. La aplicación Authenticator ahora está configurada y lista para usar.
9. Probar la autenticación:
    a. Para asegurarse de que todo esté funcionando correctamente, cierre sesión en Microsoft 365 y vuelva a iniciar sesión.
    b. Use la aplicación Authenticator para generar un código de verificación y asegúrese de que puede acceder a su cuenta.

Estos pasos le permitirán configurar y usar Microsoft Authenticator para añadir una capa adicional de seguridad a su cuenta de Microsoft 365. De la misma manera comaprto la documentación Oficial del proveedor Microsoft Usar Microsoft Authenticator con Microsoft 365. (Microsoft Corporation, 2024)

Pruebas y Validación

Realizar pruebas exhaustivas de la VPN, MFA, ingreso de los usuarios a las carpetas para verificar que los accesos funcionen adecuadamente y la segregación de permisos. Validar que todos los usuarios pueden acceder remotamente de manera segura.

ITIL 5.2.7 (Gestión de Monitoreo y Eventos): *Configurar el monitoreo de la infraestructura y los servicios de TI.*

ITIL 5.2.17 (Gestión de Pruebas y Validación): *Realizar pruebas exhaustivas para asegurar la funcionalidad y seguridad de la solución.*

Despliegue y Mantenimiento

1. Despliegue Gradual: Implementar la solución de manera gradual, comenzando con un grupo piloto para validar la funcionalidad. Recopilar feedback y realizar ajustes necesarios antes de implementar a toda la organización.

ITIL 4.3.6 (Gestión de la Implementación del Servicio): *Implementar la solución de manera controlada y gradual.*

2. Capacitación y Documentación: Proporcionar capacitación a los empleados sobre el uso de Office 365, SharePoint y la VPN. Proveer documentación de procedimientos.

   ISO/IEC 27001 (A.7.2): *Concienciación, educación y formación en seguridad de la información.*

   ITIL 5.1.4 (Gestión del Conocimiento): *Proporcionar capacitación y documentación para los usuarios finales.*

3. Monitoreo Continuo: Establecer un sistema de monitoreo continuo para supervisar la actividad de la red, el acceso a Office 365 y el rendimiento del sistema.

ITIL 5.2.7 (Gestión de Monitoreo y Eventos): *Establecer un sistema de monitoreo continuo para supervisar la infraestructura y los servicios***.**

4. Soporte Técnico Continuo: Proporcionar soporte técnico continuo para resolver problemas, realizar actualizaciones de seguridad y mantener la integridad de la infraestructura.

   ISO/IEC 27001 (A.14.1): *Requisitos de seguridad de los sistemas de información. El objetivo es garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo su ciclo de vida.*

   ITIL 5.2.5 (Gestión de Incidentes y Solicitudes): *Proveer soporte técnico continuo para resolver problemas y mantener la integridad de la infraestructura.*

GUÍA DE PRÁCTICAS RECOMENDADAS

- Mantener el Software Actualizado
    - Regularmente actualizar el software de Office 365, WatchGuard UTM y Nagios para asegurar que estén protegidos contra las últimas amenazas y vulnerabilidades.
    - Configurar actualizaciones automáticas siempre que sea posible para garantizar una protección continua.

ITIL 5.2.11 (Gestión de la Configuración y Activos de TI): *Asegurar que el software esté actualizado y protegido contra las últimas amenazas y vulnerabilidades.*

- Revisar y Actualizar Políticas
    - Revisar periódicamente las políticas de seguridad de Office 365, WatchGuard UTM y Nagios para asegurarse de que estén alineadas con las necesidades y los estándares de seguridad de la organización.
    - Ajustar las políticas según sea necesario para abordar nuevas amenazas y cambios en el entorno de seguridad.

ISO/IEC 27001 (A.5.1): *Política de seguridad de la información. Este control tiene como objetivo proporcionar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.*

- Auditorías Regulares
    - Realizar auditorías de seguridad y revisiones de la infraestructura de acceso remoto para asegurar el cumplimiento continuo con las normas ISO/IEC 27001 e ITIL.
    - Revisar la configuración de seguridad de la VPN proporcionada por WatchGuard UTM para garantizar el cumplimiento continuo con las normas de seguridad.

ISO/IEC 27001 (A.18.2): *Este control tiene como objetivo garantizar que la seguridad de la información es implementada y operada de acuerdo con las políticas y procedimientos organizacionales.*

REFERENCIAS

Microsoft Corporation. (2023, 10 25). *Niveles de permisos y permisos de usuario de SharePoint Server local*. Retrieved from Microsoft Learn: https://learn.microsoft.com/es-es/sharepoint/sites/user-permissions-and-permission-levels

Microsoft Corporation. (2024). *Crear una carpeta en una biblioteca de documentos*. Retrieved from Microsoft Support: https://support.microsoft.com/es-es/office/crear-una-carpeta-en-una-biblioteca-de-documentos-3d6a8c11-2490-4d6b-8837-f25649a69c56

Microsoft Corporation. (2024). *Usar Microsoft Authenticator con Microsoft 365*. Retrieved from Microsoft Support: https://support.microsoft.com/es-es/topic/usar-microsoft-authenticator-con-microsoft-365-1412611f-ad8d-43ab-807c-7965e5155411

Nagios. (n.d.). *Notifications*. Retrieved from Nagios Core: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/notifications.html

Nagios. (n.d.). *Quickstart Installation Guides*. Retrieved from Nagios Core: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/quickstart.html

WatchGuard. (2018). *Acerca de las Reglas y Conjuntos de Reglas*. Retrieved from Fireware Help: https://www.watchguard.com/help/docs/fireware/12/es-419/Content/es-419/proxies/general/rule_rulesets_about_c.html

WatchGuard. (2023). *Instalar el Software Cliente de WatchGuard*. Retrieved from WatchGuard Help Center: https://www.watchguard.com/help/docs/help-center/es-xl/Content/en-US/Endpoint-Security/installation/install-client-software.html?

WatchGuard. (2023). *Configurar VPN Administradas*. Retrieved from WatchGuard Help Center: https://www.watchguard.com/help/docs/help-center/es-xl/Content/en-US/Fireware/dimension/managed_vpns_configure_d.html

APÉNDICE B

Manual de Gestión de Seguridad de la Información

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA INFORMÁTICA

MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

MELANNIE ANGÉLICA MORA CORRALES

JULIO, 2024

CONTENIDOS

INTRODUCCIÓN

La seguridad de la información es un componente esencial para la protección de los activos de información en cualquier organización. Este manual ofrece una guía para la gestión de la seguridad de la información, alineada con las normas ISO/IEC 27001, ISO/IEC 27002 y las pautas de COBIT. El propósito principal es definir y documentar políticas de seguridad de la información que establezcan roles y permisos específicos para cada usuario, asegurando un acceso controlado y seguro a la información.

La implementación de estas políticas tiene como objetivo garantizar la disponibilidad, confidencialidad e integridad de los datos. Al adoptar estas normas y pautas, la organización no solo mitiga riesgos significativos, sino que también cumple con los requisitos legales y regulatorios, fomentando una cultura de seguridad en toda la empresa. Este manual proporciona las bases para un entorno de seguridad robusto y adaptable, capaz de responder eficazmente a las amenazas emergentes y proteger los activos más valiosos de la organización.

OBJETIVOS

Confidencialidad: Garantizar que la información es accesible solo para aquellos autorizados a acceder a ella.

Integridad: Salvaguardar la exactitud y completitud de la información y los métodos de procesamiento.

Disponibilidad: Asegurar que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieran.

Políticas de Control de Acceso

Objetivo

Establecer directrices y principios para proteger la información de la organización contra accesos no autorizados, modificaciones indebidas y pérdida de disponibilidad.

Alcance

Aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información de la organización.

Control de Acceso de Usuarios

- Registro de Usuarios: Implementar procesos de registro y baja de usuarios.

COBIT Proceso DSS05.03: *Gestionar la seguridad de los usuarios finales desde los puestos de trabajo del usuario final. Configurar los sistemas operativos y accesos de forma segura.*

- Gestión de Derechos de Acceso: Asignar derechos de acceso basados en roles laborales y la necesidad de saber.
- Revisión de Derechos de Acceso: Realizar revisiones periódicas para asegurarse de que los derechos de acceso sean apropiados.

Responsabilidades de organización

- Uso de Contraseñas: Implementar políticas estrictas para la creación y manejo de contraseñas.
- Autenticación de Usuarios: Usar autenticación multifactor para acceder a sistemas críticos.

COBIT Proceso DSS05.04: *Gestionar la identidad de los usuarios y el acceso lógico de los usuarios. Mantener los derechos de acceso de los usuarios de acuerdo con la función comercial, los requisitos del proceso y las políticas de seguridad. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de privilegio mínimo, necesidad de tener y necesidad de saber.*

Control de Acceso a la Red

- Segmentación de la Red: Dividir la red en segmentos separados para minimizar el acceso no autorizado.

COBIT Proceso DSS05.02: *Gestionar la seguridad de las redes y la conectividad. Permitir que solo los dispositivos autorizados tengan acceso a la información corporativa y a la red empresarial. Configure estos dispositivos para forzar la entrada de contraseña.*

- Monitoreo y Registro: Registrar y monitorear el acceso a la red y a los sistemas.

ISO/IEC 27001 (A.9.1): *Establecimiento de una política de control de acceso y procedimientos relacionados para asegurar que el acceso a los activos de información esté restringido únicamente a personas autorizadas.*

COBIT Proceso DSS05.07: *Monitorear la infraestructura para detectar eventos relacionados con la seguridad. Utilizar continuamente una cartera de tecnologías, servicios y activos compatibles (por ejemplo, escáneres de vulnerabilidades, fuzzers y sniffers, analizadores de protocolos) para identificar vulnerabilidades de seguridad de la información.*

Definición de Roles y Permisos

Identificación de Roles

Definir roles específicos dentro de la organización, basados en las responsabilidades y necesidades de acceso a la información. Los roles en esta empresa son: gerentes, recursos humanos, contabilidad, empleados de operaciones e invitado.

Responsabilidades

- Gerentes: Acceso completo a todas las áreas de información.
    - Recursos Humanos: Acceso a información relacionada con empleados, excluyendo datos financieros y estratégicos.
    - Contabilidad: Acceso a información financiera y contable.
- Empleados de Operaciones: Acceso limitado a datos necesarios para sus funciones cotidianas, sin acceso a información sensible de gerencia, recursos humanos o contabilidad.
- Invitados: Empleados temporales como practicantes, acceso limitado.

Asignación de Permisos

Asignar permisos basados en los roles identificados, asegurando que cada rol tenga el mínimo nivel de acceso necesario para cumplir con sus responsabilidades.

Administrador (Admin):

- Tiene acceso total a todos los datos y sistemas.
- Puede crear, editar, eliminar y gestionar información y usuarios.

Empleado (User):

- Tiene acceso limitado solo a la información necesaria para realizar su trabajo.
- Puede ver y editar solo sus propios datos y los relacionados con sus tareas específicas. Ejemplo: Personal de ventas, marketing, finanzas, etc. Paola, Juan y Starlyn.

Invitado (Guest):

- Tiene acceso muy limitado, generalmente solo de lectura.

- No puede editar ni eliminar información.

Matriz de Control de Accesos

Objetivo

Garantizar que el acceso a los activos de información esté restringido únicamente a personas autorizadas en función de sus roles y responsabilidades, asegurando la confidencialidad, integridad y disponibilidad de la información. Esta matriz ayuda a implementar controles adecuados para prevenir el acceso no autorizado, minimizar riesgos de seguridad y asegurar el cumplimiento de las políticas de control de acceso de la organización.

Pasos para Crear una Matriz de Accesos Basada en Roles

1. **Listar los Roles**

Descripción: En una tabla de Excel, realice una lista de los roles que existen en la empresa. Para esto, sírvase de utilizar el organigrama o las descripciones de trabajo de cada puesto. Referirse al ejemplo de la Figura 3.

Acción: Colocar la información de roles en las filas de la matriz.

2. **Agregar las Aplicaciones que Usa la Empresa**

Descripción: En las columnas de la matriz, agregue las aplicaciones y bases de datos que usa la empresa. Es recomendable listarlas todas, pero como mínimo deben figurar las que tienen información crítica o las que se hayan definido en el alcance del proyecto. Referirse al ejemplo de la Figura 3.

Acción: Asegurarse de incluir aplicaciones clave y bases de datos con información crítica.

3. **Crear el Modelo de Accesos y Permisos para Cada Rol**

Descripción: Definir un modelo a seguir de permisos y accesos para cada rol. Para este paso se debe marcar con una cruz (o cualquier otro símbolo) los permisos que idealmente deberían tener cada uno de los roles.

Acción: Asignar permisos específicos a cada rol, indicando claramente qué tipo de acceso (lectura, escritura, administración) tiene cada uno.

Figura 2

Matriz de Permisos por Usuarios

PERMISO	Admin	Empleado Operacional	Invitado
Acceso a toda la información	X		
Crear / Editar usuarios	X		
Ver información de la empresa	X	X	X
Editar datos del departamento	X	X	
Ver datos del departamento	X	X	
Crear / Editar documentos	X	X	
Ver docuementos	X	X	X

Fuente: Elaboración Propia

4. **Conocer el Panorama Real de Accesos y Permisos**

Descripción: Revisar cómo está la situación actual. Para esto se recomienda dirigirse a cada aplicación y exportar la lista de usuarios con acceso para comparar con la matriz y poder resaltar aquellos permisos que se deban corregir o agregar. Si este paso se está realizando por primera vez en la integración del sistema, podemos saltar al siguiente.

Acción: Consultar la documentación de cada aplicación para saber cómo exportar estas listas. En el caso de bases de datos, se debe realizar una consulta estándar para obtener este reporte.

5. **Configurar y Corregir los Accesos**

Descripción: Tomar las diferencias resaltadas e iniciar con la corrección de permisos o agregar los accesos y permisos necesarios no existentes. Para realizar dicha configuración o modificación de accesos en la infraestructura propuesta, siga el paso a paso que detallo a continuación:

1. Iniciar sesión en Microsoft:
    a. Vaya a Microsoft usando su navegador web.
    b. Inicie sesión con sus credenciales de administrador.
2. Acceder a la sección de Gestión de Acceso Privilegiado:

   a. En el menú de navegación izquierdo, seleccione "Gestión de Acceso Privilegiado" o "Privileged Access Management".
3. Configurar la política de acceso privilegiado:
   a. Haga clic en "Configurar política" o "Configure Policy" para comenzar la configuración.
   b. Seleccione las políticas y reglas que desea aplicar para gestionar el acceso privilegiado.
4. Definir roles y permisos:
   a. Configure los roles y permisos que se asignarán a los usuarios. Esto puede incluir la selección de roles predefinidos o la creación de roles personalizados según sus necesidades.
   b. Haga clic en "Agregar rol" o "Add Role" para añadir un nuevo rol.
   c. Complete los detalles del rol y asigne los permisos correspondientes.
5. Asignar roles a usuarios:
   a. Una vez definidos los roles, asigne estos roles a los usuarios que necesitan acceso privilegiado.
   b. Haga clic en "Asignar usuario" o "Assign User".
   c. Seleccione los usuarios y los roles que les asignará.
6. Configurar alertas y revisiones:
   a. Configure alertas para recibir notificaciones sobre actividades relacionadas con el acceso privilegiado.
   b. Establezca revisiones periódicas para asegurar que el acceso privilegiado se revisa y se ajusta regularmente.
   c. Haga clic en "Configurar alertas" o "Configure Alerts" para establecer las notificaciones.
7. Guardar y aplicar la configuración:
   a. Una vez que haya configurado las políticas, roles, permisos y alertas, haga clic en "Guardar" o "Save" para aplicar los cambios.
   b. Asegúrese de que todos los ajustes se han guardado correctamente.
8. Verificar la configuración:

   a. Revise la configuración para asegurarse de que todas las políticas de acceso privilegiado se hayan aplicado como se esperaba.
   b. Realice una prueba para confirmar que las alertas y revisiones funcionan correctamente.

9. Monitorear y ajustar:
   a. Monitoree las actividades relacionadas con el acceso privilegiado a través del panel de control de Microsoft.
   b. Ajuste las configuraciones y políticas según sea necesario para mejorar la seguridad y el cumplimiento.

Estos pasos le guiarán en la configuración de la Gestión de Acceso Privilegiado en Microsoft, ayudando a proteger el acceso a recursos críticos y a gestionar los privilegios de forma efectiva. En caso de querer consultar un paso a más detalle debe dirigirse a la documentación oficial de Office 365. Introducción a la administración del acceso con privilegios. (Microsoft, 2023)

Acción: Modificar los accesos tanto en la aplicación como en la matriz para que estén alineados.

6. Controlar Periódicamente

Descripción: Realizar controles periódicos a la matriz con una frecuencia mínima semestral o trimestral. Los startups, en particular, pueden experimentar cambios rápidos en cuanto a aplicaciones y personal.

Acción: Programar revisiones regulares para asegurar que la matriz esté actualizada y refleje la situación actual de accesos y permisos.

Figura 3

Matriz de Control de Accesos

Roles / Aplicaciones	Outlook	Word	Excel	PowerPoint	OneDrive	SharePoint	Teams	WatchGuard	Nagios
Gerentes	Admin / CRUD	Admin / CRUD	Admin / CRUD	Admin / CRUD	Admin / CRUD	Admin / CRUD	Admin / CRUD	Admin / CRUD	Admin / CRUD
Empleados Operativos	User / Read Write	User / Read Write	User / Read Write	User / Read Write	User / Read Write	User / Read Write	User / Read Write	NA	NA
Guest	Read	Read	Read	Read	Read	Read	Read Write	NA	NA

Fuente: Elaboración Propia

Políticas de Seguridad de la Información por Implementar

Provisión de Accesos

Establecer un procedimiento formal para la solicitud y aprobación de accesos a sistemas y aplicaciones. Este procedimiento debe incluir:

1. Solicitud formal del acceso, especificando el rol y nivel de acceso requerido.
2. Justificación de la solicitud del acceso respecto a las responsabilidades laborarles.
3. Revisión y aprobación por parte del supervisor directo y el administrador del sistema.
4. Configuración del acceso por parte del equipo de TI.

Para la correcta realización del plan de provisión de acceso en Office 365, refiérase al paso a paso que le detallo a continuación:

1. Iniciar sesión en Microsoft Entra:
    - Vaya a Microsoft Entra usando su navegador web.
    - Inicie sesión con sus credenciales de administrador.
2. Acceder a la sección de Gestión de Acceso:
    - En el menú de navegación izquierdo, seleccione "Gestión de Acceso" o "Access Management".
3. Definir los requisitos de acceso seguro:
    - Haga clic en "Crear nuevo plan" o "Create New Plan".
    - Especifique los objetivos y requisitos de su plan de acceso seguro, como los niveles de acceso necesarios y las condiciones de seguridad.
4. Configurar políticas de acceso:
    - Defina las políticas de acceso que determinan cómo los usuarios deben autenticarse y qué recursos pueden acceder.

- Configure las reglas de acceso basadas en la identidad, el dispositivo, la ubicación, y otros factores.
- Haga clic en "Agregar política" o "Add Policy" para añadir nuevas políticas.

5. Establecer controles de autenticación:
    - Configure los métodos de autenticación multifactor (MFA) para asegurar que los usuarios se autentiquen de manera segura.
    - Haga clic en "Configurar MFA" o "Configure MFA" y siga las instrucciones para establecer los métodos de autenticación, como mensajes de texto, aplicaciones de autenticación o biometría.
6. Aplicar el principio de menor privilegio:
    - Asegúrese de que los usuarios solo tengan acceso a los recursos necesarios para su función.
    - Revise y ajuste los permisos para garantizar que se apliquen las reglas de acceso más restrictivas posibles.
7. Configurar el acceso condicional:
    - Establezca reglas de acceso condicional para que los usuarios solo puedan acceder a recursos bajo ciertas condiciones (por ejemplo, desde una red corporativa o con un dispositivo compatible).
    - Haga clic en "Configurar acceso condicional" o "Configure Conditional Access" para definir estas reglas.
8. Monitorear y auditar el acceso:
    - Use las herramientas de monitoreo y auditoría de Microsoft Entra para revisar y analizar los accesos y las actividades.
    - Configure alertas para recibir notificaciones sobre eventos de acceso inusuales o sospechosos.

9. Revisar y ajustar el plan:
    - Revise regularmente el plan de acceso seguro para asegurarse de que sigue cumpliendo con las políticas de seguridad de su organización.
    - Ajuste las políticas y configuraciones según sea necesario para abordar nuevas amenazas o cambios en la infraestructura.
10. Comunicar a los usuarios:
    - Informe a los usuarios sobre las nuevas políticas de acceso y cómo se verán afectados.
    - Proporcione capacitación o recursos para ayudar a los usuarios a adaptarse a los cambios.

Estos pasos le ayudarán a crear y gestionar un plan de acceso seguro con Microsoft Entra, asegurando que el acceso a los recursos esté bien controlado y protegido. En caso de requerir consultar un paso a detalle, se recomienda revisar la documentación de la empresa proveedora del producto, Microsoft en la sección: Creación de un plan de seguridad para el acceso a recursos. (Microsoft, 2023)

ISO/IEC 27001 (A.9.2): *Control de acceso de los usuarios. Este control asegura que los usuarios solo puedan acceder a los sistemas y servicios necesarios para cumplir con sus funciones.*

COBIT Proceso DSS05.04: *Gestionar la identidad de los usuarios y el acceso lógico de los usuarios*

Revisión de Accesos

Realizar revisiones periódicas de los accesos para asegurar que los permisos sean apropiados y que los accesos no utilizados sean revocados. El proceso para realizar dicha revisión y su paso a paso, se presenta en detalle a continuación:

1. Iniciar sesión en Microsoft Entra:

- Vaya a Microsoft Entra usando su navegador web.
- Inicie sesión con sus credenciales de administrador.

2. Acceder a la sección de Gobernanza de Identidad:
   - En el menú de navegación izquierdo, seleccione "Gobernanza de Identidad" o "Identity Governance".
3. Configurar una revisión de acceso:
   - Haga clic en "Revisiones de acceso" o "Access Reviews".
   - Seleccione "Nueva revisión de acceso" o "New Access Review" para crear una nueva revisión.
4. Definir el alcance de la revisión:
   - Configure los parámetros de la revisión, como el grupo de usuarios, las aplicaciones o los recursos que serán revisados.
   - Haga clic en "Seleccionar recursos" o "Select Resources" y elija los elementos que desea incluir en la revisión.
5. Configurar los detalles de la revisión:
   - Establezca el título de la revisión, la frecuencia con la que debe realizarse (una vez, mensual, trimestral, etc.), y las fechas de inicio y fin.
   - Haga clic en "Configurar detalles" o "Configure Details" para ingresar esta información.
6. Seleccionar los revisores:
   - Elija las personas que serán responsables de revisar el acceso. Esto puede incluir administradores, líderes de equipo, o responsables de seguridad.
   - Haga clic en "Agregar revisores" o "Add Reviewers" y seleccione los usuarios adecuados.

7. Configurar notificaciones y recordatorios:
    - Configure las notificaciones para que los revisores reciban recordatorios sobre la revisión de acceso.
    - Haga clic en "Configurar notificaciones" o "Configure Notifications" y ajuste las opciones de acuerdo con sus necesidades.
8. Iniciar la revisión:
    - Una vez que todos los parámetros estén configurados, haga clic en "Iniciar revisión" o "Start Review" para comenzar el proceso de revisión.
    - Los revisores recibirán una notificación y podrán comenzar a evaluar los accesos.
9. Monitorear el progreso de la revisión:
    - Supervise el progreso de la revisión desde el panel de administración de Microsoft Entra.
    - Haga clic en "Ver progreso" o "View Progress" para ver cómo avanza la revisión y si hay alguna acción pendiente.
10. Revisar y aplicar los resultados:
    - Una vez que la revisión esté completa, revise los resultados y las recomendaciones.
    - Haga clic en "Ver resultados" o "View Results" para examinar las decisiones tomadas por los revisores.
    - Aplique las acciones necesarias, como revocar accesos o ajustar permisos, según los resultados de la revisión.
11. Generar informes y registrar auditoría:
    - Genere informes sobre la revisión de acceso para tener un registro de las decisiones y acciones realizadas.

- Haga clic en "Generar informe" o "Generate Report" para crear un informe detallado de la revisión.

12. Revisar y ajustar el proceso:
    - Revise el proceso de revisión de acceso para identificar áreas de mejora.
    - Ajuste las configuraciones y políticas de revisión según sea necesario para optimizar el proceso y asegurar la conformidad con las políticas de seguridad.

Estos pasos le ayudarán a gestionar de manera efectiva las revisiones de acceso en Microsoft Entra Identity Governance, garantizando que los accesos sean revisados periódicamente y que se mantenga un control adecuado sobre los permisos y accesos en su organización. De la misma manera, este proceso se puede encontrar en la documentación oficial de Microsoft. Administración del acceso de usuarios y usuarios invitados con revisiones de acceso. (Microsoft, 2024)

COBIT (Monitoreo, Evaluación y Evaluación): *COBIT establece que se debe monitorear y evaluar el desempeño del sistema de gestión de seguridad de la información. Esto incluye la supervisión de la conformidad con las políticas de seguridad y la evaluación de la efectividad de los controles implementados.*

Revocación de Accesos

Establecer un procedimiento para la revocación inmediata de accesos cuando un empleado deje la organización o cambie de rol. Así como conceder accesos de manera temporal de acuerdo con la necesidad. El proceso para realizar dicha revocación y su paso a paso lo detallo a continuación:

1. Iniciar sesión en OneDrive o SharePoint:
    - Vaya a OneDrive o SharePoint usando su navegador web.
    - Inicie sesión con su cuenta de Microsoft.
2. Encontrar el archivo o carpeta que desea modificar:
    - Navegue hasta el archivo o la carpeta que desea dejar de compartir o para la que desea cambiar los permisos.

- En OneDrive, busque el archivo o la carpeta en su lista de archivos.
- En SharePoint, navegue hasta la biblioteca de documentos donde está el archivo o carpeta.

3. Seleccionar el archivo o carpeta:
    - Haga clic en el archivo o la carpeta para seleccionarlo.
    - En OneDrive, puede hacer clic en el ícono de círculo a la izquierda del archivo o carpeta.
    - En SharePoint, seleccione el archivo o la carpeta haciendo clic en la casilla de verificación al lado del nombre.
4. Abrir el panel de detalles:
    - En OneDrive, haga clic en el ícono de "Información" (i) en la parte superior derecha para abrir el panel de detalles.
    - En SharePoint, haga clic en el botón "Información" en la barra superior o el icono de "Detalles".
5. Verificar los permisos actuales:
    - En el panel de detalles, seleccione "Administrar acceso" o "Manage Access" para ver quién tiene acceso al archivo o carpeta y qué permisos tienen.
6. Dejar de compartir o cambiar permisos:
    - Para dejar de compartir:
        - En el panel de "Administrar acceso", busque la opción "Dejar de compartir" o "Stop Sharing".
        - Haga clic en "Dejar de compartir" para revocar el acceso para todos los usuarios o grupos que no deberían tener acceso.
    - Para cambiar permisos:

- En el panel de "Administrar acceso", seleccione el usuario o grupo para el que desea cambiar los permisos.
- Haga clic en la opción de configuración de permisos (como el lápiz o "Editar").
- Cambie el tipo de acceso (por ejemplo, de "Puede editar" a "Solo ver") y guarde los cambios.

7. Confirmar los cambios:
    - Asegúrese de que los cambios se hayan aplicado correctamente.
    - Revise la lista de accesos para confirmar que los permisos se hayan actualizado como deseado.
8. Cerrar el panel de detalles:
    - Una vez que haya terminado de ajustar los permisos, puede cerrar el panel de detalles.
    - En OneDrive, haga clic en la "X" en la esquina superior derecha del panel de detalles.
    - En SharePoint, haga clic en el botón de cierre en el panel de detalles.
9. Verificar desde el archivo o carpeta:
    - Asegúrese de que el archivo o la carpeta se comporte según los cambios realizados.
    - Pruebe acceder al archivo o la carpeta con diferentes cuentas, si es necesario, para verificar los permisos.

Estos pasos le permitirán gestionar y ajustar la compartición y los permisos de archivos o carpetas en OneDrive o SharePoint, asegurando que solo las personas adecuadas tengan acceso a la información. De la misma manera se puede encontrar documentado adecuadamente en la documentación oficial de Microsoft. Dejar de compartir archivos o carpetas de OneDrive o SharePoint o cambiar los permisos. (Microsoft, 2024)

ISO/IEC 27001 (A.9.2.6): *Revocación de derechos de acceso. Este control asegura que los derechos de acceso sean removidos cuando los usuarios dejan la organización o cambian de roles.*

Autenticación y Autorización

Implementar mecanismos robustos de autenticación (por ejemplo, autenticación multifactorial) y autorización para verificar la identidad de los usuarios y controlar el acceso a los recursos. Se adjunta la documentación oficial para la integración de la aplicación de autenticación multifactor de Microsoft Office 365 llamada Authenticator. Usar Microsoft Authenticator con Microsoft 365. (Microsoft, 2024)

ISO/IEC 27001 (A.9.4): *Gestión de acceso del sistema y aplicación. Este control asegura que los usuarios sean autenticados antes de concederles acceso a los sistemas y aplicaciones.*

Monitoreo y Auditoría

Dominio COBIT Supervisión, Evaluación y Verificación. **Proceso MEA01** *Supervisar, Evaluar y Valorar*

Rendimiento y Conformidad

Establecer procesos de monitoreo y auditoría para detectar y responder a actividades sospechosas o no autorizadas, asegurando la protección continua de los activos de información. Estos procesos deben incluir:

Registro de Accesos y Actividades:

- Objetivo: Mantener un registro detallado de todos los accesos y actividades realizadas en los sistemas de información.
- Contenido:
    - Qué Registrar: Accesos exitosos y fallidos, cambios de configuración, acciones críticas como la creación o eliminación de usuarios, documentos, entre otros.
    - Herramientas: Utilizar herramientas de registro como SIEM (Security Information and Event Management) para centralizar y analizar los registros.

- Frecuencia: Registro en tiempo real.

COBIT Proceso MEA01.01: *Establecer un enfoque de monitoreo. Controlar que los procesos y las prácticas se estén desempeñando de acuerdo con los objetivos y métricas de desempeño y conformidad acordados. Proporcionar informes sistemáticos y oportunos.*

Análisis Regular de los Registros:

- Objetivo: Identificar y analizar anomalías y posibles incidentes de seguridad.
- Procedimientos: Revisiones periódicas de registros por el equipo de seguridad, o bien los gerentes, utilizando herramientas automatizadas para detectar patrones inusuales.
- Frecuencia: Semanalmente para revisiones básicas; mensual para análisis detallados.

COBIT Proceso MEA01.02: *Establecer objetivos de rendimiento y cumplimiento. Monitorear y evaluar continuamente el entorno de control, incluyendo autoevaluaciones y autoconocimiento. Permitir a la gerencia identificar deficiencias e ineficiencias de control e iniciar acciones de mejora.*

Implementación de Alertas y Notificaciones Automáticas:

- Objetivo: Proporcionar alertas en tiempo real sobre actividades sospechosas.
- Contenido:
    - Configuración de Alertas: Establecer umbrales y criterios para alertas automáticas sobre intentos de acceso no autorizados, cambios de configuración no aprobados, etc.
- Frecuencia: En tiempo real, con revisiones mensuales de la configuración de alertas.

COBIT Proceso MEA01.03: *Recolectar y procesar datos de rendimiento y conformidad.*

Auditorías Internas y Externas:

- Objetivo: Realizar auditorías regulares para evaluar la efectividad de los controles de seguridad.
- Contenido:

  - Auditorías Internas: Realizadas por el equipo de auditoría interna para revisar el cumplimiento de las políticas de seguridad, o bien los gerentes en conjunto de supervisión de un especialista en auditorías.
  - Auditorías Externas: Contratar auditores externos para una revisión independiente y objetiva.
  - Informe de Resultados: Documentar los hallazgos y recomendaciones en un informe detallado.
- Frecuencia: Anualmente para auditorías internas y bianualmente para auditorías externas.

ISO/IEC 27001 (A.12.4): *Registro y monitoreo de eventos. Este control asegura que se registren y monitoreen los eventos relevantes de seguridad de la información para identificar posibles incidentes de seguridad*

COBIT Proceso MEA01.04: *Analiza e informa sobre el rendimiento. Diseñar informes de desempeño de procesos que sean concisos, fáciles de entender y adaptados a las distintas necesidades y audiencias de la administración.*

COBIT Proceso MEA01.05: *Asegurar la implementación de acciones correctivas. Revisar las respuestas, opciones y recomendaciones de la gerencia para abordar los problemas y las principales desviaciones.*

Capacitación y Concienciación

COBIT Proceso APO07: *Gestionar recursos humanos*

Proporcionar capacitación regular a todos los empleados sobre las políticas y procedimientos de seguridad de la información. Esto debe incluir:

Concienciación sobre las Amenazas y Vulnerabilidades:

- Objetivo: Sensibilizar a los empleados sobre las amenazas de seguridad más comunes y cómo pueden afectar a la organización.
- Contenido: Presentaciones sobre phishing, malware, ingeniería social, y mejores prácticas de seguridad.
- Frecuencia: Trimestral.

Capacitación sobre el Uso Adecuado de Sistemas y Aplicaciones:

- Objetivo: Enseñar a los empleados cómo usar las herramientas y sistemas de manera segura.
- Contenido: Tutoriales y guías sobre el uso seguro de Office 365, SharePoint, y la VPN.
- Frecuencia: Al menos una vez al año o cuando se introducen nuevas herramientas.

Simulacros de Respuesta a Incidentes de Seguridad:

- Objetivo: Preparar a los empleados para responder eficazmente a incidentes de seguridad.
- Contenido: Ejercicios prácticos y simulacros de respuesta a incidentes.
- Frecuencia: Anual.

COBIT Proceso Relacionado a los 3 apartados anteriores APO07.03: *Administrar las habilidades y competencias del personal. Identificar brechas entre las habilidades requeridas y disponibles. Desarrollar planes de acción, como capacitación (habilidades técnicas y de comportamiento), reclutamiento, redistribución y estrategias de abastecimiento modificadas, para abordar las brechas a nivel individual y colectivo.*

Evaluación y Certificación:

- Objetivo: Evaluar el conocimiento de los empleados y asegurar que comprenden las políticas de seguridad.
- Contenido: Exámenes y cuestionarios después de cada sesión de capacitación.
- Frecuencia: Después de cada programa de capacitación.

ISO/IEC 27001 (A.7.2): *Concienciación, educación y formación en seguridad de la información. Este control nos pide incluir en los contratos con los empleados y subcontratas las obligaciones y responsabilidades ligadas a la Seguridad de la Información, teniendo en cuenta que muchos de los comportamientos anómalos dentro de una organización se deben a la relajación de la propia organización. Mantener informados a los trabajadores de las condiciones de trabajo es una muy buena medida preventiva de conductas indebidas para la seguridad de la información.*

Implementación y Mejora Continua

Implementación

La implementación efectiva de las políticas y procedimientos de seguridad de la información definidos en este manual es fundamental para proteger los activos de información de la organización. Asegurar que todos los empleados y partes interesadas comprendan y cumplan con las directrices establecidas es clave para el éxito de estas políticas. Este proceso debe incluir:

1. **Capacitación y Concienciación:** Realizar programas de capacitación y concienciación para todos los empleados sobre las políticas de seguridad de la información, asegurando que entiendan su papel en la protección de los datos de la organización.

ISO/IEC 27001 (A.7.2): *Concienciación, educación y formación en seguridad de la información. Este control asegura que los empleados reciban la formación adecuada sobre las políticas y procedimientos de seguridad de la información.*

2. **Comunicación:** Establecer canales de comunicación claros para que los empleados puedan reportar incidentes de seguridad y recibir actualizaciones sobre cambios en las políticas.

ISO/IEC 27001 (A.6.1.3): *Contacto con las autoridades. Este control asegura que existan procedimientos claros para el reporte y la gestión de incidentes de seguridad.*

3. **Documentación:** Asegurar que todas las políticas y procedimientos estén documentados y accesibles para todos los empleados.

ISO/IEC 27001 (A.8.1.1): *Inventario de activos. Este control asegura que toda la documentación relevante esté actualizada y disponible para los interesados.*

4. Responsabilidad y Seguimiento: Designar responsables para la implementación y el seguimiento del cumplimiento de las políticas de seguridad.

ISO/IEC 27001 (A.6.1.1): *Roles y responsabilidades en la seguridad de la información. Este control asegura que se asignen claramente las responsabilidades de la seguridad de la información.*

Mejora Continua

La mejora continua es un componente esencial de la gestión de la seguridad de la información, alineada con las normas ISO/IEC 27001 y las mejores prácticas de la ISO/IEC 27002. Establecer un ciclo de mejora continua asegura que las políticas y procedimientos se mantengan efectivos y actualizados frente a nuevos desafíos y amenazas. Este ciclo debe incluir:

- **Evaluación Periódica de Riesgos y Amenazas:** Realizar evaluaciones regulares para identificar y analizar nuevos riesgos y amenazas a la seguridad de la información, y ajustar las políticas en consecuencia.

ISO/IEC 27001 (A.6.1.2): *Gestión de riesgos de seguridad de la información. Este control asegura que los riesgos se identifiquen y gestionen adecuadamente.*

- **Revisión y Actualización de la Matriz de Roles y Permisos:** Revisar y actualizar periódicamente la matriz de roles y permisos para asegurarse de que los accesos y autorizaciones reflejen los cambios en la organización y las necesidades de seguridad.

ISO/IEC 27001 (A.9.2.3): *Gestión de derechos de acceso. Este control asegura que los derechos de acceso se gestionen y revisen periódicamente.*

- **Revisión y Ajuste de los Procedimientos de Gestión de Accesos:** Evaluar y mejorar continuamente los procedimientos de gestión de accesos, asegurando que solo el personal autorizado tenga acceso a la información crítica.

COBIT (Entrega, Servicio y Soporte – Proceso DSS05): Administración de la seguridad de la información. Este proceso asegura que los procedimientos de acceso se revisen y mejoren constantemente.

- **Incorporación de Lecciones Aprendidas de Incidentes de Seguridad y Auditorías:** Analizar los incidentes de seguridad y los resultados de las auditorías internas para identificar áreas de mejora. Las lecciones aprendidas deben incorporarse en las políticas y procedimientos para prevenir futuros incidentes.

ISO/IEC 27001 (A.16.1.6): *Lecciones aprendidas de los incidentes de seguridad. Este control asegura que las organizaciones aprendan de los incidentes para mejorar sus políticas y procedimientos.*

REFERENCIAS

Microsoft. (2023, 10 25). *Creación de un plan de seguridad para el acceso a recursos*. Retrieved from Microsoft Learn: https://learn.microsoft.com/es-es/entra/architecture/3-secure-access-plan

Microsoft. (2023, 08 21). *Introducción a la administración del acceso con privilegios*. Retrieved from Microsoft Learn: https://learn.microsoft.com/es-es/purview/privileged-access-management-configuration

Microsoft. (2024, 04 09). *Administración del acceso de usuarios y usuarios invitados con revisiones de acceso*. Retrieved from Microsoft Learn: https://learn.microsoft.com/es-es/entra/id-governance/manage-access-review

Microsoft. (2024). *Dejar de compartir archivos o carpetas de OneDrive o SharePoint o cambiar los permisos*. Retrieved from Microsoft Support: https://support.microsoft.com/es-es/office/dejar-de-compartir-archivos-o-carpetas-de-onedrive-o-sharepoint-o-cambiar-los-permisos-0a36470f-d7fe-40a0-bd74-0ac6c1e13323

Microsoft. (2024). *Usar Microsoft Authenticator con Microsoft 365*. Retrieved from Microsoft Support: https://support.microsoft.com/es-es/topic/usar-microsoft-authenticator-con-microsoft-365-1412611f-ad8d-43ab-807c-7965e5155411

Microsoft. (2024). *Usar Microsoft Authenticator con Microsoft 365*. Retrieved from Microsoft Support: https://support.microsoft.com/es-es/topic/usar-microsoft-authenticator-con-microsoft-365-1412611f-ad8d-43ab-807c-7965e5155411

APÉNDICE C

Guía de Configuración Uniforme de Medidas de Seguridad en Dispositivos

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA INFORMÁTICA

GUÍA DE CONFIGURACIÓN UNIFORME DE MEDIDAS DE SEGURIDAD EN DISPOSITIVOS

MELANNIE ANGÉLICA MORA CORRALES

JULIO, 2024

CONTENIDOS

INTRODUCCIÓN

En el mundo actual, donde las amenazas cibernéticas son cada vez más frecuentes y sofisticadas, es esencial para cualquier organización implementar medidas de seguridad uniformes y robustas para proteger sus activos de información. CORGIA Gestión e Ingeniería Alternativa, una empresa comprometida con la innovación y la excelencia operativa, reconoce la necesidad imperativa de fortalecer su postura de seguridad para salvaguardar sus datos críticos y garantizar la continuidad de sus operaciones.

Con este objetivo en mente, propongo la creación de un Manual de Configuración Uniforme de la Seguridad basado en los estándares internacionales NIST SP 800-53 e ISO/IEC 27001. Estos marcos proporcionan un conjunto de mejores prácticas y controles de seguridad ampliamente aceptados, diseñados para mitigar riesgos y asegurar que todos los dispositivos dentro de la organización operen bajo políticas de seguridad coherentes y efectivas.

Objetivos de la Guía

El Manual de Configuración Uniforme de la Seguridad se propone alcanzar los siguientes objetivos:

1. **Establecer Estándares de Seguridad Consistentes**: Implementar y mantener configuraciones de seguridad uniformes en todos los dispositivos de la empresa, siguiendo los lineamientos de NIST SP 800-53 e ISO/IEC 27001.
2. **Definir Procedimientos y Políticas Claras**: Desarrollar procedimientos detallados y políticas específicas para la instalación de antivirus, configuraciones de cortafuegos y otras medidas de seguridad esenciales.
3. **Garantizar la Coherencia y Robustez**: Asegurar una defensa coherente y robusta contra las amenazas cibernéticas mediante la aplicación sistemática de los estándares de seguridad definidos.
4. **Promover la Continuidad Operativa**: Proteger la información crítica y garantizar la continuidad operativa de CORGIA a través de prácticas de seguridad efectivas y sostenibles.

Alcance

Esta guía se aplica a todos los dispositivos de CORGIA, incluyendo estaciones de trabajo, servidores, dispositivos móviles y cualquier otro equipo que acceda a la red corporativa.

Impacto Esperado

La implementación de este manual proporcionará varios beneficios clave a CORGIA:

- **Mejora de la Postura de Seguridad**: Reducirá la probabilidad y el impacto de los incidentes de seguridad al establecer una base sólida de medidas de protección.
- **Cumplimiento Normativo**: Facilitará el cumplimiento de auditorías y normativas de seguridad, garantizando que CORGIA se mantenga alineada con las mejores prácticas internacionales.
- **Resiliencia y Continuidad**: Contribuirá a la resiliencia de la organización frente a interrupciones causadas por amenazas cibernéticas, asegurando la continuidad de las operaciones críticas.

Justificación de los Marcos NIST SP 800-53 e ISO/IEC 27001

Los marcos NIST SP 800-53 e ISO/IEC 27001 han sido seleccionados debido a su relevancia y eficacia comprobada en la gestión de la seguridad de la información:

- **NIST SP 800-53**: Proporciona una lista exhaustiva de controles de seguridad y privacidad que cubren todos los aspectos necesarios para proteger los sistemas de información y activos de la organización.
- **ISO/IEC 27001**: Establece los requisitos para un sistema de gestión de seguridad de la información (SGSI), asegurando un enfoque estructurado para la evaluación y el tratamiento de riesgos de seguridad de la información.

Políticas y Controles

Como parte de las políticas que se implementarán en la empresa, se hará uso de los controles que nos detalla NIST SP 800-53. La relevancia de estos controles se especificará en los procedimientos que se definirán en la siguiente sección de la guía, sin embargo, estos se relacionan estrechamente.

NIST SP 800-53: Control System and Information Integrity - 3 (Malicious Code Protection). Sustituya cada [Asignación] con el valor que se ha definido para CORGIA Gestión e Ingeniería Alternativa en cada control a implementar.

- Implemente mecanismos de protección contra código malicioso, en este caso el software adquirido AGV, en los puntos de entrada y salida del sistema para detectar y erradicar el código malicioso.
- Actualice automáticamente los mecanismos de protección contra código malicioso a medida que se dispongan de nuevas versiones, de acuerdo con la política y los procedimientos de gestión de configuración de la organización.
- Configure los mecanismos de protección contra código malicioso para:
    - Realizar análisis periódicos del sistema *[Asignación: frecuencia definida por la organización]* y análisis en tiempo real de archivos provenientes de fuentes externas en *[Asignación (uno o más): punto final, puntos de entrada y salida de la red]* mientras los archivos son descargados, abiertos o ejecutados, de acuerdo con la política de la organización.
    - Bloquear código malicioso, poner en cuarentena código malicioso, tomar *[Asignación: acción definida por la organización]*; y enviar alertas a *[Asignación: personal o roles definidos por la organización]* en respuesta a la detección de código malicioso.
- Abordar la recepción de falsos positivos durante la detección y erradicación de código malicioso y el impacto potencial resultante en la disponibilidad del sistema

Seguidamente, se detallan los controles que se deben implementar como parte de esta guía, que corresponden a NIST SP 800-53 System and Information Integrity - 4: Information System

Monitoring. Sustituya cada [Asignación] con el valor que se ha definido para CORGIA Gestión e Ingeniería Alternativa en cada control a implementar.

La organización:

- Monitorea el sistema de información para detectar:
    - Ataques e indicadores de posibles ataques de acuerdo con *[Asignación: objetivos de monitoreo definidos por la organización];* y
    - Conexiones locales, de red y remotas no autorizadas;
- Identifica el uso no autorizado del sistema de información a través de *[Asignación: técnicas y métodos definidos por la organización];*
- Despliega dispositivos de monitoreo:
    - Estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y
    - En ubicaciones ad hoc dentro del sistema para rastrear tipos específicos de transacciones de interés para la organización;
- Protege la información obtenida de las herramientas de monitoreo de intrusiones contra el acceso no autorizado, la modificación y la eliminación.
- Aumenta el nivel de actividad de monitoreo del sistema de información siempre que haya indicaciones de un mayor riesgo para las operaciones y activos organizacionales, individuos, otras organizaciones o la Nación basadas en información de aplicación de la ley, información de inteligencia u otras fuentes creíbles de información.
- Obtiene una opinión legal con respecto a las actividades de monitoreo del sistema de información de acuerdo con las leyes federales aplicables, órdenes ejecutivas, directivas, políticas o regulaciones.
- Proporciona *[Asignación: información de monitoreo del sistema de información definida por la organización]* a *[Asignación: personal o roles definidos por la organización]* [Selección (uno o más): según sea necesario; *[Asignación: frecuencia definida por la organización]*].

Nota: En el contexto de monitoreo de sistemas de información, las ubicaciones ad hoc pueden ser elegidas estratégicamente para enfocarse en áreas donde se sospeche o se necesite una vigilancia intensificada, como, por ejemplo:

- Segmentos críticos de la red donde se manejan datos sensibles.
- Servidores que almacenan información crucial para la operación del negocio.
- Puntos de acceso o interfaces que podrían ser vulnerables a ataques o actividades sospechosas.

Para la implementación de políticas y controles sobre el cortafuegos o bien firewall, que se estará implementando como parte de la nueva infraestructura propuesta, específicamente WatchGuard, se tomará en cuenta los controles definidos en NIST SP 800-53 Acess Control - 4: Information Flow Enforcement.

- Implementar autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas conectados basándose en *[Asignación: políticas de control de flujo de información definidas por la organización].*

El control de flujo de información regula hacia dónde puede viajar la información dentro de un sistema y entre sistemas conectados. Este control se diferencia del acceso a la información, ya que no considera los accesos posteriores a esa información. Las restricciones de control de flujo incluyen **bloquear el tráfico externo** que pretende ser interno a la organización, evitar que la información controlada para la exportación se transmita de manera clara a través de Internet, restringir las solicitudes web que no provienen del servidor proxy interno, y limitar las transferencias de información entre organizaciones basadas en estructuras de datos y contenido.

De acuerdo con la necesidad de implementación de autenticación multifactorial, Microsoft Authenticator específicamente, se contempla el control NIST SP 800-53: Control IA-2 (Identification and Authentication).

- El sistema de información identifica y autentica de manera única a los usuarios organizacionales (o procesos que actúan en nombre de los usuarios organizacionales).

Para la política de actualización de software, parches y nuevas versiones en todos los dispositivos de la organización, se incluye el control NIST SP 800-53: Control System and Information Integrity - 2 (Flaw Remediation) el mismo declara los siguientes controles para la organización. Sustituya cada [Asignación] con el valor que se ha definido para CORGIA Gestión e Ingeniería Alternativa en cada control a implementar.

- Identifica, reporta y corrige fallos en el sistema de información.
- Prueba las actualizaciones de software y firmware relacionadas con la corrección de fallos para evaluar su efectividad y posibles efectos secundarios antes de la instalación.
- Instala actualizaciones de software y firmware relevantes para la seguridad dentro de *[Asignación: período de tiempo definido por la organización]* desde la publicación de las actualizaciones; e
- Incorpora la corrección de fallos en el proceso de gestión de configuración organizacional.

Con la intención de respaldar las políticas de contraseñas, sus requisitos y frecuencia de cambio, se implementan los controles definidos en NIST SP 800-53: Control Identification and Authentication - 5 (Authenticator Management). Sustituya cada [Asignación] con el valor que se ha definido para CORGIA Gestión e Ingeniería Alternativa en cada control a implementar.

La organización gestiona los autenticadores del sistema de información mediante:

- Verificar, como parte de la distribución inicial del autenticador, la identidad del individuo, grupo, rol o dispositivo que recibe el autenticador.
- Establecer el contenido inicial del autenticador para los autenticadores definidos por la organización.
- Asegurar que los autenticadores tengan suficiente fortaleza del mecanismo para su uso previsto.
- Establecer e implementar procedimientos administrativos para la distribución inicial de autenticadores, para autenticadores perdidos/comprometidos o dañados, y para revocar autenticadores.
- Cambiar el contenido predeterminado de los autenticadores antes de la instalación del sistema de información.

- Establecer restricciones de vida útil mínimas y máximas y condiciones de reutilización para los autenticadores.
- Cambiar/actualizar los autenticadores *[Asignación: período de tiempo definido por la organización según el tipo de autenticador]*.
- Proteger el contenido del autenticador contra la divulgación y modificación no autorizadas;
- Requerir que los individuos tomen, y que los dispositivos implementen, salvaguardias específicas de seguridad para proteger los autenticadores; y
- Cambiar los autenticadores para cuentas de grupo/rol cuando cambie la membresía de esas cuentas.

Con la intención de realizar un inventario exacto de todos los activos y dispositivos que se deben de incluir en estos controles de estandarización de medidas de seguridad y en continuo monitoreo, se implementan los controles bajo la norma NIST SP 800-53: Control CM-8 (Information System Component Inventory). Sustituya cada [Asignación] con el valor que se ha definido para CORGIA Gestión e Ingeniería Alternativa en cada control a implementar.

La organización:

- Desarrolla y documenta un inventario de componentes del sistema de información que:
    - Refleja con precisión el sistema de información actual.
    - Incluye todos los componentes dentro del límite de autorización del sistema de información.
    - Está al nivel de granularidad considerado necesario para el seguimiento e informes.
    - Incluye *[Asignación: información definida por la organización considerada necesaria para lograr una rendición de cuentas efectiva de los componentes del sistema de información];* y
- Revisa y actualiza el inventario de componentes del sistema de información *[Asignación: frecuencia definida por la organización].*

Para la evaluación de riesgos asociados a cada dispositivo, se implementarán los controles definidos en la norma NIST SP 800-53: Control RA-3 (Risk Assessment). Contempla las

siguientes responsabilidades para la organización. Sustituya cada [Asignación] con el valor que se ha definido para CORGIA Gestión e Ingeniería Alternativa en cada control a implementar.

- Realiza una evaluación de riesgos que incluye:
    - Identificar amenazas y vulnerabilidades en el sistema.
    - Determinar la probabilidad y magnitud del daño debido al acceso no autorizado, uso, divulgación, interrupción, modificación o destrucción del sistema, la información que procesa, almacena o transmite, y cualquier información relacionada; y
    - Determinar la probabilidad e impacto de efectos adversos en individuos derivados del procesamiento de información personal identificable;
- Integra los resultados de la evaluación de riesgos y las decisiones de gestión de riesgos desde las perspectivas organizacional y de misión o proceso empresarial con las evaluaciones de riesgos a nivel de sistema.
- Documenta los resultados de la evaluación de riesgos en *[Asignación: planes de seguridad y privacidad, informe de evaluación de riesgos, [Asignación: documento definido por la organización]]*;
- Revisa los resultados de la evaluación de riesgos *[Asignación: frecuencia definida por la organización];*
- Disemina los resultados de la evaluación de riesgos a *[Asignación: personal o roles definidos por la organización];* y
- Actualiza la evaluación de riesgos *[Asignación: frecuencia definida por la organización]* o cuando haya cambios significativos en el sistema, su entorno de operación u otras condiciones que puedan afectar el estado de seguridad o privacidad del sistema.

Se debe determinar una lista blanca con las aplicaciones y herramientas a las que se limita acceso desde los dispositivos destinados para las labores de la organización, por lo que se contemplan los controles establecidos en la norma NIST SP 800-53: Control CM-7 (Least Functionality). Sustituya cada [Asignación] con el valor que se ha definido para CORGIA Gestión e Ingeniería Alternativa en cada control a implementar.

- Configurar el sistema para proporcionar únicamente *[Asignación: capacidades esenciales para la misión definidas por la organización]*; y
- Prohibir o restringir el uso de las siguientes funciones, puertos, protocolos, software y/o servicios*: [Asignación: funciones, puertos del sistema, protocolos, software y/o servicios prohibidos o restringidos definidos por la organización]*.

Finalmente, para abarcar las secciones de monitoreo continuo y capacitación, se incluyen los controles de la norma NIST SP 800-53: Control CA-7 (Continuous Monitoring) y NIST SP 800-53: Control AT-2 (Security Awareness Training), respectivamente, se detalla el primero con los siguientes controles. Sustituya cada [Asignación] con el valor que se ha definido para CORGIA Gestión e Ingeniería Alternativa en cada control a implementar.

La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye:

- Establecimiento de *[Asignación: métricas definidas por la organización]* a ser monitoreadas.
- Establecimiento de *[Asignación: frecuencias definidas por la organización]* para el monitoreo *y [Asignación: frecuencias definidas por la organización]* para evaluaciones que respalden dicho monitoreo.
- Evaluaciones continuas de controles de seguridad de acuerdo con la estrategia de monitoreo continuo organizacional.
- Monitoreo continuo del estado de seguridad de las métricas definidas por la organización de acuerdo con la estrategia de monitoreo continuo organizacional.
- Correlación y análisis de la información relacionada con la seguridad generada por las evaluaciones y el monitoreo.
- Acciones de respuesta para abordar los resultados del análisis de la información relacionada con la seguridad; y
- Reporte del estado de seguridad de la organización y del sistema de información a *[Asignación: personal o roles definidos por la organización] [Asignación: frecuencia definida por la organización]*.

Para la norma NIST SP 800-53: Control AT-2 (Security Awareness Training) anteriormente mencionada, se contemplan los siguientes controles.

La organización proporciona capacitación básica de concienciación sobre seguridad a los usuarios del sistema de información (incluyendo gerentes, ejecutivos senior y contratistas):

- Como parte de la capacitación inicial para nuevos usuarios;
- Cuando se requiera por cambios en el sistema de información; y
- *[Asignación: frecuencia definida por la organización]* en adelante.

Procedimientos por Integrar

Instalación de Antivirus

- **Selección del Antivirus:** Utilizar AVG para la protección de hasta 10 dispositivos, cubriendo las necesidades de antivirus, tune-up, VPN y AntiTrack.
- **Actualización Automática:** Configurar AVG para actualizar automáticamente sus bases de datos de virus y su software.

- NIST SP 800-53: Control SI-3 (Malicious Code Protection).

- ISO/IEC 27001: A.12.2.1 Controles contra el Código malicioso: *Se deberían implementar controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios.*

- **Escaneos Programados:** Establecer escaneos completos del sistema al menos una vez por semana y escaneos rápidos diarios.

- NIST SP 800-53: Control SI-4 (System Monitoring).

- ISO/IEC 27001: A.12.4.1 (Registro de Actividad y Supervisión). *Registro y gestión de eventos de actividad: Se deberían producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información.*

Configuración de Cortafuegos

- **Configuración Básica:** Asegurar que el cortafuegos esté activado en todos los dispositivos.
- **Reglas de Tráfico:** Definir y aplicar reglas estrictas de tráfico entrante y saliente, permitiendo solo las conexiones necesarias.

- NIST SP 800-53: Control AC-4 (Information Flow Enforcement).

- ISO/IEC 27001: A.13.1.1 (Gestión de la seguridad en las redes). *Controles de red: Se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones.*

- **Monitoreo:** Implementar monitoreo continuo del cortafuegos para detectar y responder a actividades sospechosas.

- NIST SP 800-53: Control SI-4 (System Monitoring).

- ISO/IEC 27001: A.12.4.1 (Registro de Actividad y Supervisión).

Medidas Esenciales Adicionales

- **Autenticación Multifactor (MFA):** Implementar MFA para el acceso a sistemas críticos y datos sensibles.

Se adjunta la documentación oficial para la integración de la aplicación de autenticación multifactor de Microsoft Office 365 llamada Authenticator. Usar Microsoft Authenticator con Microsoft 365. (Microsoft, 2024)

- NIST SP 800-53: Control IA-2 (Identification and Authentication).

- Específicamente ISO/IEC 27001: A.9.4.2 (Control de acceso a sistemas y aplicaciones). *Procedimientos seguros de inicio de sesión: Cuando sea requerido por la política de control de accesos se debería controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on.*

- **Encriptación de Datos:** Utilizar cifrado robusto (por ejemplo, AES-256) para datos en reposo y en tránsito.

A continuación, se indica un documento del proveedor oficial de la solución propuesta WatchGuard, en la que se especifican los algoritmos de cifrado, autenticación y protocolos de IPSeec, entre otros, que se utilizan en el producto. Acerca de los Algoritmos y Protocolos de IPSec. (WatchGuard, 2023).

- NIST SP 800-53: Control SC-12 (Cryptographic Key Establishment and Management).

- ISO/IEC 27001: A.10.1.1 (Controles criptográficos). *Política de uso de los controles criptográficos: Se debería desarrollar e implementar una política que regule el uso de controles criptográficos para la protección de la información.*

- **Gestión de Parches:** Implementar una política de actualización de software y parches para todos los dispositivos, asegurando que estén protegidos contra vulnerabilidades conocidas.

NIST SP 800-53: Control SI-2 (Flaw Remediation).

ISO/IEC 27001: A.12.6.1 (Gestión de la vulnerabilidad técnica). *Gestión de las vulnerabilidades técnicas: Se debería obtener información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna para evaluar el grado de exposición de la organización y tomar las medidas necesarias para abordar los riesgos asociados.*

Bloqueo de software no permitido para instalación: Implementar una política de restricción que prohíba la instalación de software no autorizado en los sistemas de información. Esta política debe incluir mecanismos de control para detectar y bloquear la instalación de software no permitido y garantizar que solo se instale software autorizado y necesario para las operaciones organizacionales.

Para realizar el bloque de aplicaciones en los dispositivos, haciendo uso de la solución WatchGuard propuesta, seguir el paso a paso que se detalla a continuación:

1. Iniciar sesión en la interfaz de administración de WatchGuard:
    - Abra su navegador web y acceda a la interfaz de administración de su dispositivo WatchGuard.
    - Ingrese la dirección IP del dispositivo en la barra de direcciones y presione Enter.
    - Inicie sesión con sus credenciales de administrador.
2. Acceder a la configuración de políticas de tráfico:
    - En el panel de navegación izquierdo, haga clic en "Políticas" o "Policies".
    - Seleccione "Políticas de tráfico" o "Traffic Policies" para acceder a la configuración relacionada con el tráfico de red.
3. Crear una nueva política de tráfico:

- Haga clic en "Agregar" o "Add" para crear una nueva política de tráfico.
- Elija "Política de acceso" o "Access Policy" en el menú de tipos de políticas.

4. Configurar los detalles de la política:
    - Ingrese un nombre descriptivo para la política, por ejemplo, "Bloquear Aplicaciones Evasivas".
    - Configure la política para que se aplique a la interfaz de red adecuada (por ejemplo, LAN a WAN).
5. Establecer las reglas de la política:
    - En la sección de reglas de la política, configure los parámetros para bloquear aplicaciones evasivas.
    - Haga clic en "Agregar regla" o "Add Rule".
    - Configure la regla para que bloquee el tráfico de las aplicaciones identificadas como evasivas.
6. Configurar la identificación de aplicaciones:
    - En la configuración de la regla, asegúrese de seleccionar "Categorías de aplicaciones" o "Application Categories".
    - Busque y seleccione las categorías de aplicaciones evasivas que desea bloquear, como aplicaciones de VPN o proxies.
7. Establecer acciones para la política:
    - Configure la acción de la política para que sea "Bloquear" o "Block".
    - Asegúrese de que la acción de la política esté configurada para denegar el acceso a las aplicaciones evasivas seleccionadas.
8. Aplicar y guardar la política:
    - Haga clic en "Guardar" o "Save" para aplicar la nueva política.

- Revise que la política esté correctamente configurada y habilitada.

9. Verificar la aplicación de la política:
    - Asegúrese de que la política se haya aplicado correctamente revisando la lista de políticas activas.
    - Realice pruebas para confirmar que las aplicaciones evasivas están bloqueadas como se espera.
10. Monitorear y ajustar la política:
    - Monitoree el tráfico y los registros para verificar que la política esté funcionando correctamente.
    - Ajuste la configuración según sea necesario para optimizar la política de bloqueo y asegurar una cobertura adecuada.

Estos pasos le guiarán en la configuración de una política de bloqueo para aplicaciones evasivas en un dispositivo WatchGuard usando Fireware, ayudando a proteger su red contra aplicaciones que intentan eludir las medidas de seguridad. De igual manera, sírvase de seguir la siguiente guía oficial del proveedor para más detalles. Bloquear Aplicaciones Evasivas. (WatchGuard, 2023)

- NIST SP 800-53: Control CM-7 (Least Functionality).

- ISO/IEC 27001: A.12.6.2 (Gestión de la vulnerabilidad técnica). *Restricciones en la instalación de software: Se deberían establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.*

Política de Contraseñas: Establecer requisitos de contraseñas fuertes y políticas de cambio regular de contraseñas.

- NIST SP 800-53: Control IA-5 (Authenticator Management).

- ISO/IEC 27001: A.9.2.4 (Gestión de acceso de usuario). *Gestión de información confidencial de autenticación de usuarios: La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado.*

Pasos de Implementación

Evaluación y Planificación

Inventario de Dispositivos

- Responsable: Equipo de IT (administrador de sistemas).
- Objetivo: Identificar todos los dispositivos que tienen acceso a la red corporativa para asegurar su gestión y protección adecuadas.

Recursos Necesarios

- Herramientas de Gestión de Activos: Utilizar software especializado en gestión de inventarios de TI (por ejemplo, Lansweeper, Spiceworks, Snipe-IT).
- Documentación de Red: Diagramas de red y mapas de topología.

Proceso de Inventario

Identificación de Dispositivos

Escaneo de Red:

- Utilizar herramientas de escaneo de red para identificar dispositivos activos en la red.
- Registrar direcciones IP, nombres de host, y otros detalles relevantes.

Revisión de Documentación Existente:

- Consultar registros y documentación previa de activos de TI.
- Actualizar información obsoleta o incompleta.

Clasificación de Activos

Categorización:

- Clasificar dispositivos por tipo (por ejemplo, servidores, estaciones de trabajo, impresoras, dispositivos móviles).
- Asignar categorías según su importancia crítica para la operación de la organización.

Atributos Clave:

- Identificar atributos clave de cada dispositivo (por ejemplo, número de serie, especificaciones técnicas, propietario).
- Registrar la ubicación física y lógica de los dispositivos.

Documentación y Mantenimiento

Creación de Registro de Activos:

- Establecer un formato estándar para el registro de activos que incluya campos como nombre del dispositivo, número de serie, fecha de adquisición, estado de mantenimiento, responsable, etc.

Actualización Regular:

- Implementar procedimientos para la actualización periódica del inventario.
- Establecer responsabilidades claras para la actualización de registros de activos.

NIST SP 800-53: Control CM-8 (Information System Component Inventory).

ISO/IEC 27001: A.8.1.1 (Responsabilidad sobre los activos). Inventario de activos: Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.

Evaluación de Riesgos

- Responsable: Equipo de seguridad de la información.
- Objetivo: Identificar y evaluar los riesgos asociados a cada dispositivo para priorizar las medidas de seguridad necesarias.

Recursos Necesarios

- Herramientas de Evaluación de Riesgos: Software de gestión de riesgos (por ejemplo, Risk Management Framework, Microsoft Azure Risk Assessment Tool).
- Documentación de Activos: Utilizar el inventario de dispositivos creado previamente.

Proceso de Evaluación de Riesgos

Identificación de Activos Críticos

Clasificación de Información

- Utilizar directrices de clasificación según ISO/IEC 27001 (A.8.2.1) para determinar la sensibilidad y criticidad de la información manejada por cada dispositivo.
- Categorizar la información en función de su valor, requisitos legales, sensibilidad y criticidad para la organización.

Identificación de Activos Críticos

- Identificar los dispositivos que manejan o tienen acceso a información clasificada como crítica o sensible.
- Priorizar estos dispositivos para una evaluación de riesgos más detallada.

Evaluación de Riesgos

Metodología de Evaluación

- Utilizar una metodología de evaluación de riesgos reconocida (por ejemplo, análisis cualitativo, cuantitativo o semicuantitativo).
- Evaluar amenazas potenciales, vulnerabilidades y posibles impactos para cada dispositivo crítico identificado.

Análisis de Riesgos

- Asignar valores numéricos o cualitativos a la probabilidad de ocurrencia y al impacto de cada riesgo identificado.
- Calcular el riesgo residual después de considerar las medidas de seguridad existentes.

Priorización de Medidas de Seguridad

- Basado en los resultados del análisis de riesgos, priorizar las medidas de seguridad necesarias para mitigar o reducir los riesgos identificados.

Documentación Final

Informe de Evaluación de Riesgos

- Documentar los resultados de la evaluación de riesgos, incluyendo los riesgos identificados, el nivel de riesgo residual y las medidas de seguridad recomendadas.
- Incorporar estos resultados en el manual de seguridad de la información de la organización.

NIST SP 800-53: Control RA-3 (Risk Assessment).

ISO/IEC 27001: A.8.2.1 (Clasificación de la información). Directrices de clasificación: La información debería clasificarse en relación con su valor, requisitos legales, sensibilidad y criticidad para la Organización.

Implementación

Despliegue de Antivirus y Cortafuegos

- Responsable: Equipo de IT (administrador de seguridad).
- Objetivo: Instalar y configurar antivirus (AVG) en todos los dispositivos y WatchGuard para proteger contra código malicioso y controlar el flujo de información.

Recursos Necesarios

- AVG Antivirus para protección contra malware. Se adjunta una guía oficial para la correcta instalación de cada uno de los productos incluidos en la licencia adquirida para la infraestructura. AVG Antivirus Products. (AGV Antivirus, 2024)

- Descargar el instalador de AVG**:**
    - Abre tu navegador web y ve al sitio web de AVG.
    - Busca la sección de descargas y selecciona "Descargar AVG Antivirus" o "Download AVG Antivirus".
    - Elige la versión adecuada para tu sistema operativo (Windows, macOS, etc.) y haz clic en "Descargar" o "Download".
    - Espera a que se descargue el archivo del instalador en tu computadora.
- Iniciar el instalador**:**

  - Navega hasta la carpeta donde se descargó el archivo del instalador (por lo general, en la carpeta de Descargas).
  - Haz doble clic en el archivo del instalador para iniciar el proceso de instalación.
- Permitir cambios en el dispositivo**:**
  - Si se te solicita, haz clic en "Sí" o "Allow" para permitir que el instalador realice cambios en tu dispositivo.
- Aceptar los términos de licencia**:**
  - En la ventana de instalación, lee los términos del acuerdo de licencia.
  - Marca la casilla para aceptar los términos y condiciones.
  - Haz clic en "Instalar" o "Install" para continuar con la instalación.
- Seleccionar tipo de instalación**:**
  - En algunas versiones, se te ofrecerán opciones de instalación (como instalación rápida o personalizada).
  - Elige la opción de instalación que prefieras. La instalación rápida suele ser la más sencilla y recomendada para la mayoría de los usuarios.
- Esperar a que se complete la instalación**:**
  - El instalador copiará los archivos necesarios y configurará el software.
  - Esto puede tomar unos minutos. Espera a que el proceso de instalación se complete.
- Reiniciar tu computadora (si se solicita):
  - En algunos casos, el instalador puede solicitar que reinicies tu computadora para completar la instalación.
  - Si se te solicita, guarda cualquier trabajo abierto y haz clic en "Reiniciar" o "Restart".
- Abrir AVG Antivirus**:**
  - Una vez que la instalación esté completa, abre el programa AVG Antivirus.
  - Puedes encontrar el ícono de AVG en el escritorio o en el menú de inicio.
- Configurar AVG Antivirus**:**
  - Al abrir AVG por primera vez, se te pedirá que realices una configuración inicial.
  - Sigue las instrucciones en pantalla para configurar el programa según tus preferencias.

- Actualizar y realizar un escaneo inicial**:**
    - Asegúrate de que AVG esté actualizado con las últimas definiciones de virus.
    - Realiza un escaneo completo de tu computadora para asegurarte de que está libre de amenazas.

Estos pasos te guiarán en el proceso de instalación de AVG Antivirus en tu computadora, asegurando que tengas la protección necesaria contra amenazas y malware.

- WatchGuard para controlar el tráfico de red, entre otras funcionalidades de protección. Se adjunta guía oficial del proveedor para su correcta instalación y configuración. Set Up WatchGuard EDR Core. (WatchGuard, 2024)

Proceso de Implementación

Instalación de Antivirus (AVG)

- Descargar e instalar AVG Antivirus en todos los dispositivos según las licencias adquiridas y los requisitos de la organización.

Configuración Inicial

- Configurar AVG para realizar análisis programados, actualizaciones automáticas de definiciones de virus y escaneos en tiempo real.
- Asegurar que la configuración cumpla con las políticas de seguridad definidas.

Instalación de WatchGuard EDR

- Descargar e instalar WatchGuard EDR según las licencias adquiridas y los requisitos de la organización.

Configuración de Reglas

- Definir y configurar reglas de cortafuegos para controlar el tráfico de red entrante y saliente. Se adjunta guía de configuración de reglas para el software adquirido WatchGuard EDR. Configure Firewall Policies in WatchGuard Cloud. (WatchGuard, 2024)

NIST SP 800-53: Control SI-3 (Malicious Code Protection), AC-4 (Information Flow Enforcement).

ISO/IEC 27001: A.12.2.1 (Controls against malware), A.13.1.1 (Network controls).

Configuración de MFA y Encriptación

- Responsable: Equipo de seguridad de la información.
- Objetivo: Mejorar la autenticación y seguridad de acceso mediante la implementación de MFA y garantizar el cifrado adecuado de los datos sensibles.

Recursos Necesarios

- Microsoft Authenticator: Herramienta para implementar MFA.
- Herramientas de Cifrado: WatchGuard funcionalidades IPSec, cifrado, entre otras.

Implementación de MFA con Microsoft Authenticator

Configuración de Microsoft Authenticator:

- Descargar e instalar Microsoft Authenticator en todos los dispositivos según la política de seguridad. Set up multifactor authentication for Microsoft 365. (Microsoft Support, 2024)
- Configurar MFA para todos los usuarios que acceden a sistemas críticos o datos sensibles.
- Descargar Microsoft Authenticator:
    - Vaya a la tienda de aplicaciones de su dispositivo móvil (App Store para iOS o Google Play Store para Android).
    - Busque "Microsoft Authenticator" y descárguelo.
    - Instale la aplicación en su dispositivo móvil.
- Iniciar sesión en Microsoft 365:
    - Abra su navegador web y vaya a Microsoft 365.
    - Inicie sesión con su cuenta de Microsoft 365.
- Acceder a la configuración de seguridad:
    - Haga clic en su foto de perfil en la esquina superior derecha.
    - Seleccione "Ver cuenta" o "Account".
- Configurar verificación en dos pasos:

    - En el panel de navegación, haga clic en "Seguridad" o "Security".
    - Seleccione "Métodos de verificación" o "Sign-in options".
- Agregar un método de autenticación:
    - Haga clic en "Agregar método" o "Add method".
    - En el menú desplegable, seleccione "Aplicación de autenticación" o "Authenticator app".
    - Haga clic en "Agregar" o "Add".
- Configurar la aplicación Authenticator:
    - Abra la aplicación Microsoft Authenticator en su dispositivo móvil.
    - Toque el símbolo de "+" para agregar una nueva cuenta.
    - Seleccione "Cuenta personal" o "Cuenta de trabajo o escuela".
    - Si se le pide, escanee el código QR que aparece en su pantalla de Microsoft 365 usando la aplicación Authenticator.
- Confirmar la configuración:
    - Después de escanear el código QR, la aplicación Authenticator generará un código de verificación.
    - Ingrese el código de verificación en el sitio de Microsoft 365 para completar la configuración.
- Guardar y confirmar:
    - Una vez ingresado el código, haga clic en "Verificar" o "Verify" en Microsoft 365.
    - La aplicación Authenticator ahora está configurada y lista para usar.
- Probar la autenticación:
    - Para asegurarse de que todo esté funcionando correctamente, cierre sesión en Microsoft 365 y vuelva a iniciar sesión.
    - Use la aplicación Authenticator para generar un código de verificación y asegúrese de que puede acceder a su cuenta.

Estos pasos le permitirán configurar y usar Microsoft Authenticator para añadir una capa adicional de seguridad a su cuenta de Microsoft 365.

Registro y Configuración de Usuarios:

- Registrar a los usuarios en Microsoft Authenticator.
- Configurar políticas de seguridad que requieran MFA para iniciar sesión en sistemas y aplicaciones.

NIST SP 800-53: Control IA-2 (Identification and Authentication), **SC-12** (Cryptographic Key Establishment and Management).

ISO/IEC 27001: A.9.4.2 (Secure log-on procedures), A.10.1.1 (Policy on the use of cryptographic controls).

Verificación y Mantenimiento

Auditorías Regulares

Realizar auditorías de seguridad trimestrales para asegurar el cumplimiento continuo de los estándares de seguridad.

- Responsable: Equipo de auditoría interna, seguridad de la información y gerentes de área.
- Objetivo: Verificar el cumplimiento continuo de las políticas de seguridad y detectar posibles vulnerabilidades y áreas de mejora.

Recolección de Información

- Recopilar documentación relevante, como políticas de seguridad, procedimientos operativos y registros de cumplimiento.
- Realizar entrevistas con el personal clave y observar los procedimientos en acción.

Evaluación Técnica

- Utilizar herramientas de auditoría para escanear sistemas y redes en busca de vulnerabilidades.
- Revisar configuraciones de seguridad y realizar pruebas de penetración si es necesario.

Verificación de Cumplimiento:

- Comparar las prácticas actuales con las políticas y normas establecidas.

Documentación de Resultados

Elaborar el Informe de Auditoría

- Documentar hallazgos, incluyendo áreas de incumplimiento, vulnerabilidades y riesgos identificados.
- Proporcionar recomendaciones claras y prácticas para mitigar los riesgos y mejorar el cumplimiento.

Revisión y Validación

- Revisar el informe con los gerentes y el equipo de seguridad de la información.
- Validar los hallazgos y obtener acuerdos sobre las acciones correctivas.

Implementación de Acciones Correctivas

Plan de Acción

- Desarrollar un plan de acción para abordar los hallazgos de la auditoría.
- Asignar responsabilidades y establecer plazos para la implementación de las medidas correctivas.

Seguimiento

- Realizar seguimientos periódicos para asegurar que las acciones correctivas se implementen de manera efectiva.
- Documentar los progresos y resolver cualquier problema pendiente.

NIST SP 800-53: Control CA-7 (Continuous Monitoring).

ISO/IEC 27001: A.18.2.2 *(Revisiones de la seguridad de la información). Cumplimiento de las políticas y normas de seguridad: Los gerentes deberían revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente.*

Capacitación Continua

Proporcionar capacitación regular a los empleados sobre las mejores prácticas de seguridad y las políticas establecidas.

NIST SP 800-53: Control AT-2 (Security Awareness Training).

ISO/IEC 27001: A.7.2.2 (Information security awareness, education, and training).

REFERENCIAS

AGV Antivirus. (2024). *Support for Windows Products*. Retrieved from AGV Support: https://support.avg.com/support_win?l=en

Microsoft. (2024). *Usar Microsoft Authenticator con Microsoft 365*. Retrieved from Microsoft Support: https://support.microsoft.com/es-es/topic/usar-microsoft-authenticator-con-microsoft-365-1412611f-ad8d-43ab-807c-7965e5155411

Microsoft Support. (2024, 02 22). *Set up multifactor authentication for Microsoft 365*. Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide

WatchGuard. (2023). *Acerca de los Algoritmos y Protocolos de IPSec*. Retrieved from WatchGuard Help Center: https://www.watchguard.com/help/docs/help-center/es-xl/Content/en-US/Fireware/mvpn/general/ipsec_algorithms_protocols_c.html

WatchGuard. (2023). *Bloquear Aplicaciones Evasivas*. Retrieved from WatchGuard Help Center: https://www.watchguard.com/help/docs/help-center/es-xl/Content/en-US/Fireware/configuration_examples/block_evasive_apps_example.html

WatchGuard. (2024). *Configure Firewall Policies in WatchGuard Cloud*. Retrieved from WatchGuard Support: https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/WG-Cloud/Devices/managed/firewall_policies_configure.html

WatchGuard. (2024). *Quick Start Set Up WatchGuard EDR Core*. Retrieved from WatchGuard Support: https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/services/edr_core/edr_core_quick_start_c.html

APÉNDICE D

Guía de Gestión de Copias de Seguridad

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA INFORMÁTICA

GUÍA DE GESTIÓN DE COPIAS DE SEGURIDAD

MELANNIE ANGÉLICA MORA CORRALES

JULIO, 2024

CONTENIDOS

INTRODUCCIÓN

En el contexto empresarial actual, la gestión eficaz de la seguridad de la información y la continuidad operativa son pilares fundamentales para el éxito y la resiliencia organizacional. Para abordar correctamente problemas que impidan esta continuidad operativa, es imprescindible desarrollar una guía integral que contemple estrategias sólidas para la realización periódica y automatizada de copias de seguridad de datos críticos, basadas en normas internacionales como ISO/IEC 27001, ISO/IEC 27002 e ITIL. Esta guía no solo debe considerar la importancia de la segmentación eficiente de datos según su criticidad para la continuidad del negocio, sino también diseñar procedimientos de prueba que validen la efectividad de los respaldos.

Además, se requiere un plan estratégico que simplifique la aplicación de estas normas en la infraestructura organizacional futura, asegurando que el personal esté capacitado y consciente de las políticas de seguridad. En este sentido, la implementación de una infraestructura tecnológica avanzada y segura no solo optimizará los procesos operativos, sino que también fortalecerá la seguridad de la información, permitiendo a CORGIA adaptarse rápidamente a las demandas cambiantes del entorno empresarial y ofreciendo servicios de alta calidad en el sector de consultorías eléctricas.

Esta guía está diseñada para proporcionar a CORGIA una hoja de ruta clara y estructurada para mejorar su gestión de copias de seguridad, garantizando la protección y disponibilidad de sus datos críticos y, en última instancia, fortaleciendo su posición competitiva en el mercado.

OBJETIVOS

La Guía de Gestión de Copias de Seguridad se propone alcanzar los siguientes objetivos:

- **Establecer Estándares de Respaldo Consistentes:** Implementar y mantener configuraciones uniformes para la realización de copias de seguridad en todos los sistemas críticos de la empresa, siguiendo los lineamientos de ISO/IEC 27001, ISO/IEC 27002 y las mejores prácticas de ITIL.
- **Definir Procedimientos y Políticas Claras:** Desarrollar procedimientos detallados y políticas específicas para la segmentación de datos, la programación de respaldos y la recuperación de información, asegurando la coherencia y robustez de las copias de seguridad.
- **Garantizar la Integridad y Disponibilidad:** Asegurar que las copias de seguridad sean integras y estén disponibles para su restauración cuando sea necesario, mediante la implementación de pruebas periódicas y auditorías de los procesos de respaldo.
- **Promover la Continuidad Operativa:** Proteger la información crítica y garantizar la continuidad operativa de CORGIA a través de prácticas de respaldo y recuperación efectivas y sostenibles.
- **Capacitar al Personal:** Asegurar que el personal esté adecuadamente capacitado y consciente de las políticas de seguridad y respaldo, fomentando una cultura organizacional que priorice la protección de los datos.

Alcance

Esta guía se aplica a todos los dispositivos de CORGIA, incluyendo estaciones de trabajo, servidores, dispositivos móviles y cualquier otro equipo que acceda a la red corporativa. Esto abarca tanto dispositivos internos como externos que interactúan con los datos críticos de la organización, asegurando que todas las áreas de la infraestructura tecnológica estén protegidas y respaldadas adecuadamente.

Impacto Esperado

La implementación de esta guía proporcionará varios beneficios clave a CORGIA:

- **Protección de Datos Críticos:** Garantizará que los datos críticos de la empresa estén protegidos contra pérdidas accidentales, fallos de hardware, ataques cibernéticos y desastres naturales.
- **Disponibilidad y Recuperación:** Asegurará que la información respaldada esté disponible para su restauración rápida y efectiva, minimizando el tiempo de inactividad y los impactos operativos en caso de incidentes.
- **Cumplimiento Normativo:** Facilitará el cumplimiento de auditorías y normativas de seguridad, garantizando que CORGIA se mantenga alineada con las mejores prácticas internacionales y las regulaciones de protección de datos.
- **Optimización de Recursos:** Mediante la automatización de los procesos de respaldo y la segmentación eficiente de datos, se optimizará el uso de los recursos de almacenamiento y se reducirán los costos asociados.
- **Confianza del Cliente:** Al demostrar un enfoque proactivo y robusto hacia la protección de datos, CORGIA podrá aumentar la confianza de sus clientes en su capacidad para manejar y proteger información sensible.
- **Mejora de la Postura de Seguridad:** Al establecer procesos estandarizados para copias de seguridad, se reducirá el riesgo de pérdida de datos y se fortalecerá la seguridad general de la información en la organización.

POLÍTICAS Y CONTROLES

ISO/IEC 27001 A.8

El objetivo principal es que la organización tenga conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos. Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una política predeterminada por la propia organización. Se debería considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden resultar poco prácticos.

ISO/IEC 27001 A.8.2 Clasificación de la información

El objetivo es el de asegurar que se aplica un nivel de protección adecuado a la información.

- **A.8.2.1 Directrices de clasificación:** *La información debería clasificarse en relación con su valor, requisitos legales, sensibilidad y criticidad para la Organización.*
- **A.8.2.2 Etiquetado y manipulado de la información:** *Se debería desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la organización.*
- **A.8.2.3 Manipulación de activos:** *Se deberían desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización.*

ISO/IEC 27002 A. 8.2 CLASIFICACIÓN DE LA INFORMACIÓN

Objetivo: Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.

8.2.1 Clasificación de la información

La información debe ser clasificada en términos de requisitos legales, valor, criticidad y sensibilidad a la divulgación o modificación no autorizada.

Guía de implementación

- Las clasificaciones y los controles de protección asociados para la información deben tener en cuenta las necesidades comerciales para compartir o restringir la información, así como los requisitos legales. Otros activos además de la información también pueden clasificarse conforme a la clasificación de la información que se almacena, procesa o maneja de otra manera o se protege con el activo.
- Los propietarios de los activos de información deben ser responsables de su clasificación.
- El esquema de clasificación debe incluir convenciones para la clasificación y criterios para la revisión de la clasificación con el tiempo. El nivel de protección en el esquema debe evaluarse mediante el análisis de la confidencialidad, integridad y disponibilidad, así como cualquier otro requisito considerado para la información. El esquema debe estar alineado con la política de control de acceso.
- Cada nivel debe recibir un nombre que tenga sentido en el contexto de la aplicación del esquema de clasificación.
- El esquema debe ser consistente en toda la organización para que todos clasifiquen la información y los activos relacionados de la misma manera, tengan una comprensión común de los requisitos de protección y apliquen la protección adecuada.
- La clasificación debe incluirse en los procesos de la organización, y ser consistente y coherente en toda la organización. Los resultados de la clasificación deben indicar el valor de los activos según su sensibilidad y criticidad para la organización, por ejemplo, en términos de confidencialidad, integridad y disponibilidad. Los resultados de la clasificación deben actualizarse de acuerdo con los cambios en su valor, sensibilidad y criticidad a lo largo de su ciclo de vida.

Otra información

La clasificación proporciona a las personas que manejan información una indicación concisa de cómo manejarla y protegerla. Crear grupos de información con necesidades de protección similares y especificar procedimientos de seguridad de la información que se apliquen

a toda la información en cada grupo facilita esto. Este enfoque reduce la necesidad de evaluaciones de riesgo caso por caso y el diseño personalizado de controles.

La información puede dejar de ser sensible o crítica después de cierto tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta, ya que la sobre clasificación puede llevar a la implementación de controles innecesarios que resulten en gastos adicionales; por otro lado, la subclasificación puede poner en peligro el logro de los objetivos comerciales.

Un ejemplo de un esquema de clasificación de confidencialidad de la información podría basarse en cuatro niveles como los siguientes:

- La divulgación no causa daño.
- La divulgación causa una ligera vergüenza o inconveniente operativo menor.
- La divulgación tiene un impacto significativo a corto plazo en las operaciones u objetivos tácticos.
- La divulgación tiene un impacto grave en los objetivos estratégicos a largo plazo o pone en riesgo la supervivencia de la organización.

8.2.2 Etiquetado de la información

Debe desarrollarse e implementarse un conjunto apropiado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de información adoptado por la organización.

Guía de implementación

- Los procedimientos para el etiquetado de información deben cubrir la información y sus activos relacionados en formatos físicos y electrónicos.
- El etiquetado debe reflejar el esquema de clasificación establecido en el control anterior 8.2.1. Las etiquetas deben ser fácilmente reconocibles.

- Los procedimientos deben proporcionar orientación sobre dónde y cómo se adjuntan las etiquetas, considerando cómo se accede a la información o se manejan los activos según los tipos de medios.
- Los procedimientos pueden definir casos en los que se omite el etiquetado, por ejemplo, el etiquetado de información no confidencial para reducir la carga de trabajo.
- Los empleados y contratistas deben estar conscientes de los procedimientos de etiquetado.
- Las salidas de sistemas que contienen información clasificada como sensible o crítica deben llevar una etiqueta de clasificación apropiada.

Otra información

El etiquetado de la información clasificada es un requisito clave para los acuerdos de intercambio de información. Las etiquetas físicas y los metadatos son una forma común de etiquetado.

El etiquetado de la información y sus activos relacionados a veces puede tener efectos negativos. Los activos clasificados son más fáciles de identificar y, en consecuencia, de robar por parte de personas internas o atacantes externos.

ISO/IEC 27001 A.12.3 Gestión de Seguridad

El control de la realización de las copias de resguardo de información, así como la prueba periódica de su restauración permiten garantizar la restauración de las operaciones en los tiempos de recuperación establecidos y acotar el periodo máximo de pérdida de información asumible para cada organización.

- **A.12.3.1 Copias de seguridad de la información:** *Se deberían realizar y pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación con una política de respaldo (Backup) convenida.*

ISO/IEC 27002 A.12.3 BACKUP

12.3.1 Respaldo de la información

Deben realizarse y probarse regularmente copias de respaldo de la información y de las imágenes del sistema.

Guía de implementación

- Se debe establecer una política de respaldo para definir los requisitos de la organización en cuanto a los respaldos.
- La política de respaldo debe definir los requisitos de retención y protección.
- Se deben proporcionar instalaciones adecuadas de respaldo para garantizar que toda la información y el software esenciales puedan recuperarse tras un desastre o una falla en los medios.
- Al diseñar un plan de respaldo, se deben tener en cuenta los siguientes elementos:
    - Se deben producir registros precisos y completos de las copias de respaldo y procedimientos documentados de restauración.
    - La extensión (por ejemplo, respaldo completo o diferencial) y la frecuencia de los respaldos deben reflejar los requisitos comerciales de la organización, los requisitos de seguridad de la información implicada y la criticidad de la información para la operación continua de la organización.
    - Las copias de respaldo deben almacenarse en una ubicación remota, a una distancia suficiente para evitar cualquier daño por un desastre en el sitio principal.
    - La información de respaldo debe recibir un nivel adecuado de protección física y ambiental, consistente con los estándares aplicados en el sitio principal.
    - Los medios de respaldo deben probarse regularmente para garantizar que se pueda confiar en ellos para su uso en emergencias cuando sea necesario; esto debe combinarse con una prueba de los procedimientos de restauración y verificarse contra el tiempo de restauración requerido. La prueba de la capacidad de restaurar datos respaldados debe realizarse en medios de prueba dedicados, no sobrescribiendo los medios originales en caso de que el proceso de respaldo o restauración falle y cause daños irreparables o pérdida de datos.
    - En situaciones donde la confidencialidad es importante, las copias de respaldo deben protegerse mediante cifrado.

- Los procedimientos operativos deben monitorear la ejecución de los respaldos y abordar los fallos de los respaldos programados para asegurar la integridad de los respaldos de acuerdo con la política de respaldo.
- Los arreglos de respaldo para sistemas y servicios individuales deben probarse regularmente para garantizar que cumplen con los requisitos de los planes de continuidad del negocio. En el caso de sistemas y servicios críticos, los arreglos de respaldo deben cubrir toda la información del sistema, aplicaciones y datos necesarios para recuperar el sistema completo en caso de un desastre.
- El período de retención para la información comercial esencial debe determinarse, teniendo en cuenta cualquier requisito de que las copias de archivo se conserven de forma permanente.

ITIL IT Infraestructura Library

ITIL (IT Infrastructure Library, biblioteca de infraestructura de TI) es un Marco de referencia que describe un conjunto de mejores prácticas y recomendaciones para la administración de servicios de TI, con un enfoque de administración de procesos.

Según ITIL V3.0, Marco de buenas prácticas:

"La copia de seguridad y restauración es esencialmente un componente del buen servicio de TI. Como tal, el diseño debe garantizar que haya una copia de seguridad sólida, las estrategias para cada servicio y la transición del servicio deben garantizar que estos sean debidamente probados."

"Los datos de la organización deben estar protegidos y esto incluirá respaldo(copia) y almacenamiento de datos en ubicaciones remotas donde se puede proteger – y ser usados en caso de que necesite ser restaurado debido a pérdida, corrupción o implementación de TI en planes de continuidad del servicio."

Se debe acordar una estrategia general de respaldo, que abarque:

- La información que se va a respaldar, la frecuencia y los intervalos en los que se deben hacer las copias de seguridad.

- El tipo de copia de seguridad (completa, parcial, incremental) y los puntos de verificación que se utilizarán.
- Las ubicaciones que se usarán para el almacenamiento.
- Pruebas / comprobaciones a realizar, como lecturas de prueba y restauraciones de prueba.
- Objetivo del punto de recuperación. Esto describe el punto al cual los datos serán restaurados después de la recuperación.
- Objetivo de tiempo de recuperación. Esto describe el tiempo máximo permitido para recuperación después de una interrupción.
- Cómo verificar que las copias de seguridad funcionarán si es necesario restaurarlas. Los procedimientos de respaldo deben incluir un paso de verificación para garantizar que las copias de seguridad estén completas y que funcionarán si se necesita una restauración.
- Es necesario adquirir y gestionar los medios necesarios (discos, cintas, CD, etc.) que se utilizarán para copias de seguridad, para que no haya escasez de suministros.
- Cuando se utilizan dispositivos automatizados, la precarga de los medios necesarios debe ser por adelantado. Al cargar y borrar medios devueltos desde fuera del sitio almacenamiento es importante que haya un procedimiento para verificar que estos son los correctos. Esto evitará que se sobrescriba la copia de seguridad más reciente con fallas de datos, y luego no tener datos válidos para restaurar.
- Las copias de seguridad deben ser generadas de forma automática.
- Si las copias de seguridad se automatizan o se realizan de forma remota, entonces la supervisión de eventos y capacidades deben ser consideradas para que cualquier falla pueda ser detectada de manera temprana y ser rectificadas antes de que causen problemas.
- En todos los casos, el personal de Operaciones de TI debe estar capacitado en respaldo (y restauración), los procedimientos deben estar bien documentados en las operaciones de TI de la organización (Manual de Procedimientos)

PROCEDIMIENTOS

Evaluación y Planificación

Identificación y Clasificación de Datos

- Responsable: Gerentes de la empresa en conjunto con administrador TI.
- Objetivo: Identificar y clasificar la información de la organización basándose en su criticidad y sensibilidad para implementar las medidas de protección adecuadas.
- **ITIL 5.2.15 Service Level Management:** *establecer objetivos claros basados en el negocio para los niveles de servicio y garantizar que la prestación de servicios se evalúe, controle y gestione adecuadamente en relación con estos objetivos.*

Recursos Necesarios

- Herramientas de Clasificación de Datos: Software de clasificación de datos (por ejemplo, Varonis, Netwrix).
- Documentación de Políticas: Políticas de seguridad de la información, manuales y guías de clasificación.
- Formación del Personal: Programas de capacitación para la correcta identificación y clasificación de datos.

- **ITIL 5.2.6 IT Asset Management:** *planificar y gestionar el ciclo de vida completo de todos los activos de TI, para ayudar a la organización a: maximizar el valor, controlar los costos, gestionar los riesgos, respaldar la toma de decisiones sobre la compra, reutilización, retiro y disposición de activos, y cumplir con los requisitos regulatorios y contractuales.*

Proceso de Clasificación de datos

Identificación de Activos de Información

- Inventario de Datos: Crear un inventario detallado de todos los activos de información dentro de la organización, incluyendo documentos, correos electrónicos, bases de datos, etc.

- Revisión de Documentación Existente: Consultar registros y documentación previa de activos de TI para actualizar información obsoleta o incompleta.
- **ITIL 5.2.11 Service Configuration Management:** *garantizar que la información precisa y confiable sobre la configuración de los servicios y los elementos de configuración que los respaldan esté disponible cuando y donde se necesite.*

Definición de Criterios de Clasificación

- Categorías de Datos: Definir las categorías de datos basadas en su criticidad y sensibilidad (por ejemplo, críticos, sensibles, no críticos).
- Parámetros de Clasificación: Establecer los parámetros para cada categoría, como el impacto potencial en caso de divulgación, pérdida o corrupción.
- ISO/IEC 27002 A. 8.2 CLASIFICACIÓN DE LA INFORMACIÓN
- **ITIL 5.1.3 Information Security Management:** *Proteger la información que la organización necesita para llevar a cabo sus actividades. Esto incluye comprender y gestionar los riesgos a la confidencialidad, integridad y disponibilidad de la información.*

Asignación de Clasificaciones

- Etiquetado de Datos: Asignar etiquetas de clasificación a los datos según los criterios definidos. Utilizar herramientas automatizadas para aplicar estas etiquetas donde sea posible.
- Revisión y Validación: Los gerentes y el administrador TI deben revisar y validar las clasificaciones asignadas para asegurar su precisión.
- **ITIL 5.1.3 Information Security Management.**

Frecuencia y Programación de Respaldo

- Responsable: Administrador TI en conjunto con el equipo de seguridad de la información.
- Objetivo: Establecer una política de copias de seguridad que defina la frecuencia y programación de los respaldos según la criticidad de los datos para garantizar su integridad y disponibilidad.

- **ITIL 5.2.1 Availability Management:** Garantizar que los servicios ofrezcan niveles de disponibilidad acordados para satisfacer las necesidades de los clientes y usuarios.

Recursos Necesarios

- Software de Respaldo: Herramientas de respaldo automatizadas (por ejemplo, Veeam para Microsoft Office 365, Acronis, Backup Exec). About Veeam Backup for Microsoft 365 (Veeam, 2024)
- Infraestructura de Almacenamiento: Espacio de almacenamiento adecuado para copias de seguridad, incluyendo almacenamiento local y en la nube. Microsoft 365 Backup. (Microsoft Corporation, 2024)
- Documentación de Políticas: Políticas de respaldo y recuperación documentadas y accesibles.

- **ITIL 5.2.3 Capacity and Performance Management:** Garantizar que los servicios alcancen el rendimiento acordado y esperado, satisfaciendo la demanda actual y futura de manera rentable

Proceso de Frecuencia y Programación de Respaldo

Evaluación de la Criticidad de los Datos

- Clasificación de Datos: Basarse en la clasificación de datos para determinar la criticidad y sensibilidad de la información.
- Identificación de Datos Críticos: Identificar qué datos son esenciales para las operaciones de la organización y requieren respaldos más frecuentes.

- **ITIL 5.2.1 Availability Management**

Definición de la Frecuencia de Respaldo

- Datos Críticos: Establecer respaldos diarios para datos críticos que son esenciales para la continuidad del negocio.

- Datos Sensibles: Programar respaldos semanales para datos sensibles que son importantes, pero no críticos.
- Datos No Críticos: Realizar respaldos mensuales para datos que no son críticos y pueden ser recuperados con menor urgencia.

- **ITIL 5.2.12 Service Continuity Management:** *Garantizar que la disponibilidad y el rendimiento de un servicio se mantengan en niveles suficientes en caso de desastre.*

Automatización de Respaldo

- Configuración de Herramientas: Configurar herramientas automatizadas de respaldo para ejecutar copias de seguridad en las frecuencias definidas.
- Monitoreo Automatizado: Implementar sistemas de monitoreo para asegurar que los respaldos se realicen correctamente y sin intervención manual.

Programación de Respaldo

- Calendario de Respaldo: Crear y mantener un calendario de respaldos detallado que especifique las fechas y horas de los respaldos programados.
- Ventanas de Respaldo: Definir ventanas de tiempo para realizar respaldos fuera de las horas pico de operación para minimizar el impacto en el rendimiento del sistema.

- **ITIL 5.2.3 Capacity and Performance Management**

Verificación y Pruebas de Respaldo

- Pruebas Regulares: Realizar pruebas periódicas de restauración de datos para verificar la integridad y disponibilidad de los respaldos.
- Documentación de Pruebas: Mantener un registro detallado de todas las pruebas de respaldo y restauración, incluyendo los resultados y cualquier problema identificado.

- **ITIL 5.2.12 Service Continuity Management**

ISO/IEC 27001 (A.8.1.1): *Inventario de activos. Este control asegura que toda la documentación relevante esté actualizada y disponible para los interesados.*

Revisión y Actualización de Políticas

- Auditorías Periódicas: Realizar auditorías periódicas para revisar la efectividad de la política de respaldos y hacer ajustes según sea necesario.
- Mejoras Continuas: Actualizar las políticas y procedimientos de respaldo basados en los resultados de las auditorías y en cambios en las necesidades de la organización.

Notificación y Alerta

Alertas Automatizadas: Configurar alertas automatizadas para notificar al equipo de TI y a los gerentes sobre el estado de los respaldos y cualquier error que ocurra durante el proceso.

- Iniciar sesión en Nagios Log Server:
    - Abre tu navegador web y accede a la interfaz de Nagios Log Server usando la dirección IP o el nombre de dominio de tu servidor.
    - Inicia sesión con tus credenciales de administrador.
- Acceder a la sección de Alertas:
    - En el panel de navegación, haz clic en "Alertas" o "Alerts".
- Crear una nueva alerta:
    - Haz clic en "Agregar alerta" o "Add Alert" para iniciar la configuración de una nueva alerta.
- Definir los parámetros de la alerta:
    - **Nombre de la alerta**: Ingresa un nombre descriptivo para la alerta.
    - **Tipo de alerta**: Selecciona el tipo de alerta que deseas configurar, como "Basado en eventos" o "Event-Based".
- Configurar los criterios de la alerta:
    - **Filtro de eventos**: Define los criterios para los eventos que activarán la alerta. Puedes usar filtros basados en palabras clave, niveles de severidad, o patrones específicos en los registros.
    - **Ejemplo de filtro**: Si deseas alertar sobre eventos de error, puedes configurar un filtro que busque la palabra "ERROR" en los registros.
- Establecer la frecuencia de notificación:

  - Configura la frecuencia con la que se enviarán las notificaciones de alerta.
  - Puedes elegir notificar cada vez que ocurra el evento o establecer un intervalo de tiempo específico para las notificaciones.
- Configurar los métodos de notificación:
  - **Correo electrónico**: Ingresa las direcciones de correo electrónico a las que se enviarán las notificaciones de alerta.
  - **Otros métodos**: Configura otros métodos de notificación disponibles, como mensajes SMS, integraciones con herramientas de terceros, o sistemas de mensajería.
- Establecer el umbral de alerta:
  - Define el umbral que debe alcanzarse para que se genere una alerta. Esto puede incluir la cantidad de eventos que deben ocurrir en un periodo de tiempo determinado.
  - Ejemplo: Puedes configurar la alerta para que se active si hay más de 10 eventos de error en una hora.
- Guardar y activar la alerta:
  - Revisa la configuración de la alerta para asegurarte de que todo esté configurado correctamente.
  - Haz clic en "Guardar" o "Save" para guardar la configuración de la alerta.
  - Asegúrate de que la alerta esté activada para que comience a monitorear los eventos de registro.
- Verificar el funcionamiento de la alerta:
  - Realiza una prueba para asegurarte de que la alerta se activa como se espera.
  - Puedes generar un evento que coincida con los criterios de la alerta para verificar que se envíen las notificaciones correctamente.
- Monitorear y ajustar las alertas:
  - Monitorea el funcionamiento de las alertas desde el panel de "Alertas" en Nagios Log Server.
  - Ajusta los criterios, umbrales, o métodos de notificación según sea necesario para optimizar la efectividad de las alertas.

Estos pasos te guiarán en la configuración de alertas basadas en eventos de registro con Nagios Log Server, ayudando a mantenerte informado sobre eventos críticos y asegurando una respuesta rápida a posibles problemas. Alerting On Log Events (Nagios, 2021)

Informes Periódicos: Generar informes periódicos sobre el estado de los respaldos y compartirlos con la administración para garantizar la transparencia y la supervisión.

Procedimientos de Prueba de Respaldo

- Responsable: Administrador TI en conjunto con el equipo de seguridad de la información.
- Objetivo: Validar periódicamente la integridad y disponibilidad de los datos respaldados mediante pruebas de restauración, asegurando que los procesos de respaldo sean confiables y efectivos, así como garantizar que las copias de seguridad pueden ser restauradas correctamente y que los datos están intactos y accesibles.

- **ITIL 5.2.12 Service Continuity Management**

Recursos Necesarios

- Software de Restauración: Herramientas de restauración de datos (por ejemplo, Veeam, Acronis, Backup Exec).
- Ambientes de Prueba: Espacios de almacenamiento y servidores dedicados para pruebas de restauración.
- Documentación de Procedimientos: Manuales y guías detalladas de los procedimientos de restauración.

Proceso de Prueba de Respaldo

Planificación de Pruebas de Restauración

- Calendario de Pruebas: Establecer un calendario regular para la realización de pruebas de restauración (mensuales, trimestrales, anuales) según criticidad de datos.
- Selección de Datos: Seleccionar aleatoriamente datos críticos, sensibles y no críticos para las pruebas de restauración.

- **ITIL 5.2.12 Service Continuity Management**

Preparación de la Prueba

- Identificar el Tipo de Respaldo a Probar: Seleccionar entre respaldos completos, incrementales o diferenciales.
- Seleccionar Datos a Restaurar: Elegir una muestra representativa de los datos respaldados, incluyendo archivos críticos y no críticos.
- Documentar el Proceso: Registrar el propósito de la prueba, el alcance, los datos seleccionados y los recursos necesarios.

- **ITIL 5.2.12 Service Continuity Management**

Realización de la Restauración

- Acceder a la Herramienta de Respaldo: Iniciar sesión en la herramienta de respaldo utilizada Microsoft Office 365.
- Seleccionar el Respaldo a Restaurar: Navegar y seleccionar el archivo o conjunto de archivos específicos que se van a restaurar.
- Elegir el Destino de la Restauración: Determinar si se restaurarán en su ubicación original o en una ubicación alternativa para evitar sobrescribir datos actuales.
- Iniciar el Proceso de Restauración: Ejecutar la restauración siguiendo las instrucciones de la herramienta de respaldo.

Verificación de la Restauración

- Comprobar la Integridad de los Datos: Asegurarse de que los archivos restaurados están completos y no corrompidos.
- Validar la Funcionalidad: Abrir y utilizar los archivos restaurados para garantizar que funcionan correctamente.
- Documentar Resultados: Registrar los resultados de la prueba, incluyendo cualquier error encontrado y las acciones tomadas para corregirlos.

- **ITIL 5.2.12 Service Continuity Management**

Evaluación y Mejora

- Evaluar el Proceso de Restauración: Analizar la eficiencia y eficacia del proceso de restauración.
- Identificar Áreas de Mejora: Notar cualquier problema o área que pueda mejorarse en futuros respaldos.
- Actualizar Procedimientos: Modificar y mejorar los procedimientos de respaldo y restauración basándose en los hallazgos de la prueba.
- **ITIL 4.6 Continual Improvement:** *Definir la visión de la iniciativa. Esto proporciona contexto para todas las decisiones posteriores y vincula las acciones individuales con la visión de la organización para el futuro.*

Frecuencia de Pruebas

Objetivo: Asegurar que las pruebas de restauración se realizan con regularidad para mantener la confiabilidad de las copias de seguridad.

Recomendaciones para la Frecuencia de Pruebas de Restauración

- Respaldo Completo: Probar la restauración completa de datos al menos una vez al trimestre.
- Respaldo Incremental: Probar la restauración incremental al menos una vez al mes.
- Respaldo Diferencial: Probar la restauración diferencial al menos cada dos meses.
- Datos Críticos: Para datos críticos, realizar pruebas de restauración mensualmente o con mayor frecuencia si es posible.
- Datos No Críticos: Realizar pruebas de restauración de datos no críticos al menos una vez cada seis meses.

Criterios para Considerar una Prueba como Exitosa

- Integridad de los Datos
    - Todos los archivos y datos restaurados deben estar completos y sin corrupción.

    - No deben faltar archivos que estaban incluidos en el respaldo.
- Funcionalidad
    - Los archivos restaurados deben abrirse y funcionar correctamente.
    - Las aplicaciones asociadas deben reconocer y manejar los datos restaurados sin errores.
- Tiempo de Restauración
    - El tiempo necesario para completar la restauración debe estar dentro de los límites aceptables definidos en las políticas de la organización.
    - Las pruebas deben documentar el tiempo de inicio y finalización de la restauración.

Documentación y Reporte de Resultados

- Registro Detallado: Mantener un registro detallado de cada prueba de restauración, incluyendo:
    - Fecha y hora de la prueba.
    - Tipo de datos restaurados.
    - Resultados de la prueba (éxito o fracaso).
    - Problemas encontrados y acciones correctivas.
- Informe Periódico: Generar informes periódicos para la administración, detallando los resultados de las pruebas y cualquier incidencia.

Almacenamiento y Seguridad de los Respaldos

- Responsable: Administrador TI en conjunto con el equipo de seguridad de la información.
- Objetivo: Asegurar que las copias de seguridad se almacenen de manera segura, tanto físicamente como lógicamente, y se retengan según los requisitos legales y operativos.

Recursos Necesarios

- Sistemas de Almacenamiento Seguro: Dispositivos de almacenamiento físico (bóvedas, centros de datos fuera del sitio) y almacenamiento en la nube.
- Cifrado de Datos: Herramientas y tecnologías de cifrado robusto para proteger los datos respaldados. Cifrado en Microsoft 365. (Microsoft, 2023)

- Políticas de Retención de Datos: Documentos que describen las políticas de retención de datos, basados en las normativas legales y las necesidades de la organización.

- Iniciar sesión en Microsoft**:**
    - Abra su navegador web y acceda a Microsoft sitio oficial.
    - Inicie sesión con sus credenciales de administrador.
- Acceder al Centro de Cumplimiento**:**
    - En el panel de navegación izquierdo, seleccione "Centro de cumplimiento" o "Compliance Center".
- Ir a la sección de Políticas de Retención**:**
    - Dentro del Centro de Cumplimiento, busque y seleccione "Políticas de retención" o "Retention policies".
- Crear una nueva política de retención**:**
    - Haga clic en "Crear política" o "Create policy" para iniciar el proceso de creación de una nueva política de retención.
- Configurar los detalles de la política**:**
    - **Nombre de la política**: Ingrese un nombre descriptivo para la política de retención.
    - **Descripción**: Añada una descripción opcional para explicar el propósito de la política.
- Seleccionar el tipo de retención**:**
    - Elija el tipo de retención que desea aplicar, como "Conservar por un período específico" o "Conservar hasta que se elimine".
- Definir los criterios de retención**:**
    - **Período de retención**: Establezca la duración durante la cual los elementos deben ser retenidos (por ejemplo, 1 año, 7 años).
    - **Fecha de inicio**: Defina cuándo comienza el período de retención (puede ser desde la fecha de creación, la última modificación, etc.).
- Aplicar la política a ubicaciones específicas**:**
    - Seleccione las ubicaciones donde desea aplicar la política de retención, como buzones de correo, sitios de SharePoint, o OneDrive.

    - Haga clic en "Elegir ubicaciones" o "Choose locations" y seleccione las ubicaciones deseadas.
- Configurar las acciones de retención**:**
    - Defina qué acciones se deben tomar una vez que el período de retención haya terminado. Esto puede incluir la eliminación automática de elementos o la conservación indefinida.
    - Haga clic en "Configurar acciones" o "Configure actions" y ajusta las opciones según tus necesidades.
- Revisar y guardar la política**:**
    - Revise todos los detalles de la política para asegurarse de que están configurados correctamente.
    - Haga clic en "Guardar" o "Save" para guardar la configuración de la política de retención.
- Aplicar y activar la política**:**
    - Asegúrese de que la política esté activada para que comience a aplicarse a las ubicaciones seleccionadas.
    - Verifique que la política esté listada en el panel de políticas de retención activas.
- Monitorear la aplicación de la política**:**
    - Supervise la aplicación de la política desde el Centro de Cumplimiento para asegurarse de que se esté aplicando correctamente.
    - Puede revisar los informes y registros para confirmar que los elementos están siendo retenidos y gestionados según la política.
- Ajustar la política según sea necesario**:**
    - Si es necesario, ajuste los parámetros de la política de retención para optimizar su aplicación.
    - Puede editar o actualizar la política desde el panel de políticas de retención en cualquier momento.

Estos pasos ayudarán a configurar y gestionar los ajustes de retención en Microsoft, asegurando que los datos se conserven y gestionen de acuerdo con las políticas de retención de tu organización.

Configuración normal para directivas de retención y directivas de etiquetas de retención (Microsoft Corporation, 2024)

- **ITIL 5.1.3 Information Security Management:** *Proteger la información que la organización necesita para llevar a cabo sus negocios.*

Proceso de Almacenamiento y Seguridad de los Respaldos

Seguridad Física y Lógica

- Ubicación Segura: Almacenar las copias de seguridad en ubicaciones seguras, como bóvedas fuera del sitio y centros de datos con altos estándares de seguridad.
- Cifrado de Datos: Implementar cifrado robusto para los datos respaldados, asegurando que solo el personal autorizado pueda acceder a ellos.

Gestión de Retención de Datos

- Políticas de Retención: Definir y documentar políticas de retención de datos que determinen el período durante el cual los respaldos deben conservarse.
- Cumplimiento Legal: Asegurarse de que las políticas de retención cumplan con los requisitos legales y regulatorios aplicables.

Monitoreo y Auditoría

- Monitoreo Continuo: Implementar sistemas de monitoreo para asegurar que las copias de seguridad se realicen y almacenen según lo planificado.
- Auditorías Periódicas: Realizar auditorías regulares para revisar la efectividad de las políticas de seguridad y retención de los respaldos.

Acceso y Recuperación

- Control de Acceso: Establecer controles estrictos de acceso para garantizar que solo el personal autorizado pueda recuperar o gestionar los respaldos.

- Procedimientos de Recuperación: Documentar y entrenar al personal en los procedimientos de recuperación de datos desde los respaldos, asegurando una respuesta rápida y efectiva en caso de necesidad. Seguir el siguiente paso a paso que se detalla:
    1. Iniciar sesión en Microsoft 365**:**
        - Abra su navegador web y vaya a Microsoft 365.
        - Inicie sesión con sus credenciales de administrador.
    2. Acceder al Centro de Administración de Microsoft 365**:**
        - Una vez que esté en la página principal, haga clic en el ícono de "Aplicaciones" (los nueve puntos en la esquina superior izquierda).
        - Seleccione "Administrador" o "Admin" para ir al Centro de Administración.
    3. Ir a la sección de Copias de Seguridad**:**
        - En el panel de navegación izquierdo, seleccione "Mostrar todo" para ver más opciones.
        - Desplácese hacia abajo y seleccione "Copia de seguridad" o "Backup".
    4. Configurar la copia de seguridad para OneDrive y SharePoint**:**
        - **OneDrive**:
            - En la sección de OneDrive, seleccione "Configurar copia de seguridad" o "Set up backup".
            - Siga las instrucciones para configurar las copias de seguridad automáticas de los archivos en OneDrive.
        - **SharePoint**:
            - En la sección de SharePoint, seleccione "Configurar copia de seguridad" o "Set up backup".
            - Siga las instrucciones para configurar las copias de seguridad automáticas de los sitios y bibliotecas de documentos en SharePoint.
    5. **Realizar una copia de seguridad manual**:
        - **OneDrive**:
            - Abra OneDrive desde el navegador web.
            - Seleccione los archivos o carpetas que desee respaldar.

        - Haga clic en "Descargar" para guardar una copia local en su computadora.
    - **SharePoint**:
        - Abra el sitio de SharePoint desde el navegador web.
        - Navegue a la biblioteca de documentos.
        - Seleccione los archivos o carpetas que desee respaldar.
        - Haga clic en "Descargar" para guardar una copia local en su computadora.
6. **Restaurar datos desde una copia de seguridad**:
    - **OneDrive**:
        - Abra OneDrive desde el navegador web.
        - Seleccione la opción "Papelera de reciclaje" o "Recycle bin" en el panel izquierdo.
        - Seleccione los archivos o carpetas que desee restaurar y haga clic en "Restaurar" o "Restore".
    - **SharePoint**:
        - Abra el sitio de SharePoint desde el navegador web.
        - Navegue a la biblioteca de documentos.
        - Seleccione "Papelera de reciclaje" o "Recycle bin" en el panel izquierdo.
        - Seleccione los archivos o carpetas que desee restaurar y haga clic en "Restaurar" o "Restore".
7. **Configurar la retención y recuperación de datos**:
    - En el Centro de Administración de Microsoft 365, seleccione "Centro de Cumplimiento" o "Compliance Center".
    - Configure las políticas de retención para asegurar que los datos se conserven durante el tiempo necesario y estén disponibles para restauración cuando sea necesario.
8. **Monitorear y revisar las copias de seguridad**:

- Revise regularmente el estado de las copias de seguridad y asegúrese de que se estén realizando correctamente.
- Acceda a los informes de copia de seguridad para verificar que todos los datos importantes estén respaldados.

9. **Actualizar y ajustar las configuraciones de copia de seguridad**:
    - Si es necesario, ajuste las configuraciones de copia de seguridad para incluir nuevos archivos, carpetas o sitios.
    - Asegúrese de que las políticas de copia de seguridad y restauración estén actualizadas y alineadas con los requisitos de su organización.
10. **Entrenar a los usuarios sobre las prácticas de copia de seguridad y restauración**:
    - Proporcione a los usuarios guías y capacitación sobre cómo realizar copias de seguridad y restaurar sus propios datos en OneDrive y SharePoint.
    - Asegúrese de que comprendan la importancia de las copias de seguridad y sepan cómo acceder y utilizar las herramientas disponibles.

Estos pasos le guiarán en la configuración de copias de seguridad y restauración de datos en Microsoft 365, asegurando que sus archivos y datos importantes estén protegidos y sean recuperables en caso de pérdida o eliminación. Restauración de datos en Copia de seguridad Microsoft 365. (Microsoft Corporation, 2024)

REFERENCIAS

Microsoft. (2023, 09 08). *¿Qué es el cifrado y cómo funciona en Microsoft 365?* Retrieved from Microsoft Learn: https://learn.microsoft.com/es-es/purview/encryption#what-is-encryption-and-how-does-it-work-in-microsoft-365

Microsoft Corporation. (2024, 05 06). *Configuración normal para directivas de retención y directivas de etiquetas de retención*. Retrieved from Microsoft Learn: https://learn.microsoft.com/es-es/purview/retention-settings

Microsoft Corporation. (2024). *Microsoft 365 Backup*. Retrieved from Micrrosoft Adoption: https://adoption.microsoft.com/en-us/microsoft-365-backup/

Microsoft Corporation. (2024, 04 13). *Restauración de datos en Copia de seguridad Microsoft 365*. Retrieved from Microsoft Learn: https://learn.microsoft.com/es-es/microsoft-365/backup/backup-restore-data?view=o365-worldwide&tabs=onedrive

Nagios. (2021, July). *Alerting On Log Events*. Retrieved from Nagios Log Server: https://assets.nagios.com/downloads/nagios-log-server/docs/Alerting-On-Log-Events-With-Nagios-Log-Server.pdf

Veeam. (2024, 01 26). *About Veeam Backup for Microsoft 365*. Retrieved from Veeam Help Center: https://helpcenter.veeam.com/docs/vbo365/guide/vbo_introduction.html?ver=70

APÉNDICE E

Manual de Gestión de Incidentes y Auditorías Internas

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA INFORMÁTICA

MANUAL DE GESTIÓN DE INCIDENTES Y AUDITORÍAS INTERNAS

MELANNIE ANGÉLICA MORA CORRALES

JULIO, 2024

CONTENIDOS

INTRODUCCIÓN

En el contexto actual de la gestión de la seguridad de la información, la norma ISO/IEC 27001 proporciona un marco fundamental para garantizar la protección de los activos de información crítica. Este manual está diseñado para orientar a CORGIA en la gestión efectiva de incidentes de seguridad y la realización de auditorías internas, conforme a los principios y requisitos establecidos en la norma mencionada.

Las organizaciones, al manejar una cantidad considerable de activos de información, enfrentan constantemente amenazas que pueden comprometer la confidencialidad, integridad y disponibilidad de dicha información. Es esencial establecer responsabilidades claras y procedimientos eficaces para la gestión de incidentes, así como aplicar un proceso de mejora continua para evaluar, monitorear y gestionar integralmente la seguridad de la información.

Además, la recolección adecuada de evidencias es crucial para respaldar el cumplimiento de los requisitos legales y normativos pertinentes. Este enfoque sistemático no solo fortalece la capacidad de CORGIA para proteger sus activos críticos de información, sino que también asegura su alineación con las mejores prácticas internacionales en seguridad de la información según las normas internacionales.

Objetivos de la Guía

El objetivo principal de este manual es asegurar que los eventos de seguridad de la información y las vulnerabilidades asociadas a los sistemas de información sean identificados, tratados y comunicados de manera oportuna y efectiva. Esto incluye la aplicación de acciones correctivas adecuadas para mitigar los impactos potenciales y prevenir la recurrencia de incidentes similares:

1. **Establecer un Marco Estructurado:** Proporcionar un marco detallado y estructurado para la gestión de incidentes de seguridad de la información y la planificación de auditorías internas en CORGIA. Esto asegura que la organización cuente con procedimientos claros y consistentes para manejar incidentes y evaluar la efectividad del Sistema de Gestión de Seguridad de la Información (SGSI).
2. **Promover la Respuesta Eficiente a Incidentes:** Facilitar la detección temprana, evaluación rápida y respuesta efectiva a incidentes de seguridad de la información. Esto incluye la implementación de acciones correctivas y preventivas oportunas para minimizar el impacto y prevenir la recurrencia de incidentes similares en el futuro.
3. **Garantizar la Mejora Continua:** Aplicar un enfoque de mejora continua en la gestión de incidentes y auditorías internas. Esto implica la evaluación regular de procesos, políticas y controles de seguridad para identificar áreas de mejora y optimización en el SGSI.
4. **Cumplimiento con Normativas y Estándares:** Asegurar el cumplimiento con las normativas y estándares internacionales, particularmente con los requisitos establecidos por ISO/IEC 27001 e ISO/IEC 27002. Esto incluye la recolección adecuada de evidencias para demostrar la conformidad y la capacidad de enfrentar auditorías externas de manera efectiva.
5. **Protección de Activos de Información:** Fortalecer la capacidad de CORGIA para proteger sus activos críticos de información contra amenazas internas y externas. Esto se logra mediante la implementación de controles de seguridad efectivos y la respuesta proactiva a incidentes.
6. **Optimización de Recursos:** Utilizar de manera eficiente los recursos humanos y tecnológicos disponibles para la gestión de incidentes y la realización de auditorías

internas. Esto garantiza que los recursos se asignen de manera adecuada para mantener la seguridad de la información de manera sostenible.

Alcance

El alcance de la guía de gestión de incidentes y auditorías internas en CORGIA abarca los siguientes aspectos:

- **Sistemas y Procesos Involucrados:** Esta guía se aplica a todos los sistemas y procesos dentro de CORGIA que manejen información sensible y crítica para la operación diaria. Esto incluye estaciones de trabajo, servidores, dispositivos móviles y cualquier otro equipo que acceda a la red corporativa.
- **Gestión de Incidentes de Seguridad de la Información:** Establece procedimientos claros y responsabilidades definidas para la detección, manejo y reporte de incidentes de seguridad. Se enfoca en asegurar que todos los incidentes sean tratados de manera oportuna y efectiva, minimizando el impacto en la confidencialidad, integridad y disponibilidad de la información.
- **Auditorías Internas:** Define el proceso para la planificación, ejecución y seguimiento de auditorías internas. Estas auditorías evalúan la efectividad del Sistema de Gestión de Seguridad de la Información (SGSI), asegurando el cumplimiento de los requisitos normativos y facilitando la mejora continua del sistema.
- **Cumplimiento Normativo**: Garantiza que CORGIA cumpla con las normativas y estándares internacionales, particularmente con los requisitos especificados en ISO/IEC 27001:2022. Esto incluye la recolección adecuada de evidencias para demostrar la conformidad y facilitar auditorías externas.
- **Mejora Continua:** Promueve un enfoque de mejora continua en la gestión de la seguridad de la información. Esto implica la evaluación regular de procesos, políticas y controles de seguridad para identificar oportunidades de mejora y optimización en el SGSI.

Políticas y Controles

La norma ISO/IEC 27001 en el apartado 16, indica los siguientes controles, en los que se basará este manual para su correcta realización y cumplimiento:

ISO/IEC 27001 A.16.1 Gestión de incidentes de seguridad de la información y mejoras: El objetivo es asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información incluyendo la comunicación de los eventos de seguridad y debilidades.

- **16.1.1 Responsabilidades y procedimientos:** *Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.*
- **16.1.2 Notificación de los eventos de seguridad de la información:** *Los eventos de seguridad de la información se deberían informar lo antes posible utilizando los canales de administración adecuados.*
- **16.1.3 Notificación de puntos débiles de la seguridad:** *Se debería requerir anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la organización.*
- **16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones:** *Se deberían evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes.*
- **16.1.5 Respuesta a los incidentes de seguridad:** *Se debería responder ante los incidentes de seguridad de la información en atención a los procedimientos documentados.*
- **16.1.6 Aprendizaje de los incidentes de seguridad de la información**: *Se debería utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro.*
- **16.1.7 Recopilación de evidencias:** *La organización debería definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.*

Procedimientos

16.1.1 Responsabilidades y procedimientos

Control: Las responsabilidades y procedimientos de gestión deben establecerse para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.

Guía de implementación: Se deben considerar las siguientes pautas para las responsabilidades y procedimientos de gestión en relación con la gestión de incidentes de seguridad de la información:

1. Los procedimientos de gestión de incidentes de seguridad de la información deben ser desarrollados y comunicados adecuadamente dentro de la organización. Los siguientes procedimientos deben considerarse:
    a) Procedimientos para la planificación y preparación de la respuesta a incidentes;
    b) Procedimientos para la monitorización, detección, análisis y reporte de eventos e incidentes de seguridad de la información;
    c) Procedimientos para el registro de actividades de gestión de incidentes;
    d) Procedimientos para el manejo de evidencias forenses;
    e) Procedimientos para la evaluación y toma de decisiones sobre eventos de seguridad de la información y evaluación de debilidades de seguridad de la información;
    f) Procedimientos para la respuesta, incluyendo aquellos para la escalada, recuperación controlada de un incidente y comunicación a personas u organizaciones internas y externas;
2. Los procedimientos establecidos deben asegurar que:
    a) Personal competente maneje los asuntos relacionados con incidentes de seguridad de la información dentro de la organización;
    b) Se implemente un punto de contacto para la detección y reporte de incidentes de seguridad;
    c) Se mantengan contactos apropiados con autoridades, grupos de interés externos o foros que manejen asuntos relacionados con incidentes de seguridad de la información;

3. Los procedimientos de reporte deben incluir:
    a) Preparación de formularios de reporte de eventos de seguridad de la información para apoyar la acción de reporte y ayudar a la persona que reporta a recordar todas las acciones necesarias en caso de un evento de seguridad de la información;
    b) El procedimiento por seguir en caso de un evento de seguridad de la información, por ejemplo, anotar todos los detalles inmediatamente, como el tipo de incumplimiento o violación, malfuncionamiento ocurrido, mensajes en la pantalla e informar inmediatamente al punto de contacto y tomar solo acciones coordinadas;
    c) Referencia a un proceso disciplinario formal establecido para tratar con empleados que cometan violaciones de seguridad;
    d) Procesos de retroalimentación adecuados para asegurar que las personas que reportan eventos de seguridad de la información sean notificadas de los resultados después de que el asunto haya sido tratado y cerrado.

Otra información: Los incidentes de seguridad de la información pueden trascender las fronteras organizacionales y nacionales. Para responder a tales incidentes, existe una creciente necesidad de coordinar la respuesta y compartir información sobre estos incidentes con organizaciones externas según sea apropiado.

16.1.2 Reporte de eventos de seguridad de la información

Control: Los eventos de seguridad de la información deben ser reportados a través de los canales de gestión apropiados tan pronto como sea posible.

Guía de implementación: Todos los empleados y contratistas deben ser conscientes de su responsabilidad de reportar eventos de seguridad de la información tan pronto como sea posible. También deben estar al tanto del procedimiento para reportar eventos de seguridad de la información y el punto de contacto al cual deben ser reportados los eventos.

Situaciones por considerar para el reporte de eventos de seguridad de la información incluyen:

a) Control de seguridad inefectivo;
b) Violación de las expectativas de integridad, confidencialidad o disponibilidad de la información;
c) Errores humanos;
d) Incumplimientos de políticas o directrices;
e) Violaciones de los arreglos de seguridad física;
f) Cambios no controlados en el sistema;
g) Fallos de software o hardware;
h) Violaciones de acceso.

Otra información: Las fallas o comportamientos anómalos del sistema pueden ser un indicador de un ataque de seguridad o una violación de seguridad real y, por lo tanto, siempre deben ser reportados como un evento de seguridad de la información.

16.1.3 Reporte de debilidades en la seguridad de la información

Control: Se debe requerir a los empleados y contratistas que usan los sistemas y servicios de información de la organización que tomen nota y reporten cualquier debilidad en la seguridad de la información observada o sospechada en sistemas o servicios.

Guía de implementación: Todos los empleados y contratistas deben reportar estos asuntos al punto de contacto, en este caso Gerencia, tan pronto como sea posible para prevenir incidentes de seguridad de la información. El mecanismo de reporte debe ser lo más fácil, accesible y disponible posible.

Otra información: Se debe aconsejar a los empleados y contratistas que no intenten probar las debilidades de seguridad sospechadas. Probar debilidades podría interpretarse como un uso indebido potencial del sistema y también podría causar daños al sistema de información o servicio y resultar en responsabilidad legal para la persona que realiza la prueba.

16.1.4 Evaluación y decisión sobre eventos de seguridad de la información

Control: Se deben evaluar los eventos de seguridad de la información y decidir si deben clasificarse como incidentes de seguridad de la información.

Guía de implementación: El punto de contacto debe evaluar cada evento de seguridad de la información utilizando la escala de clasificación de eventos e incidentes de seguridad de la información acordada y decidir si el evento debe clasificarse como un incidente de seguridad de la información. La clasificación y priorización de incidentes puede ayudar a identificar el impacto y la extensión de un incidente.

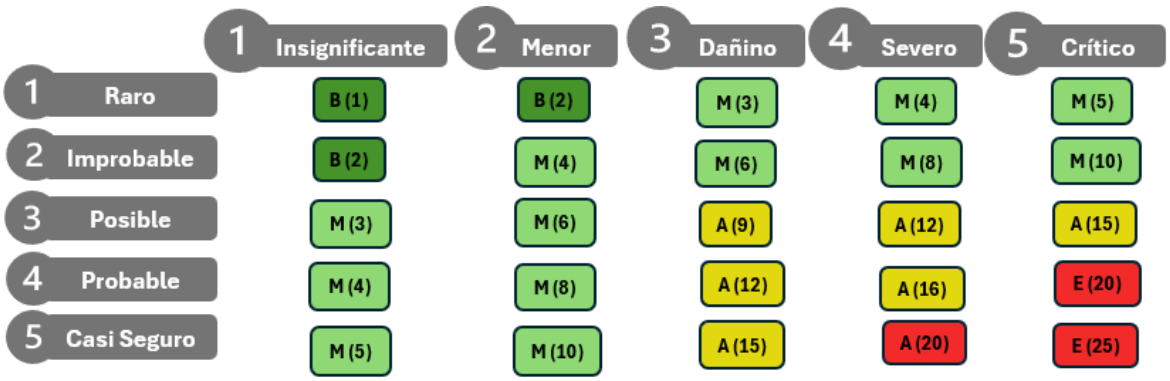
En los casos en que la organización cuente con un equipo de respuesta a incidentes de seguridad de la información (ISIRT), la evaluación y decisión pueden ser remitidas al ISIRT para confirmación o reevaluación.

Los resultados de la evaluación y decisión deben registrarse en detalle con el propósito de referencia futura y verificación.

El riesgo para categorizar dichos incidentes se calcula con la siguiente fórmula: **Probabilidad x Impacto = Riesgo.** Como se puede observar y guiar de acuerdo con las Figuras 4 y 5 a continuación:

Figura 4

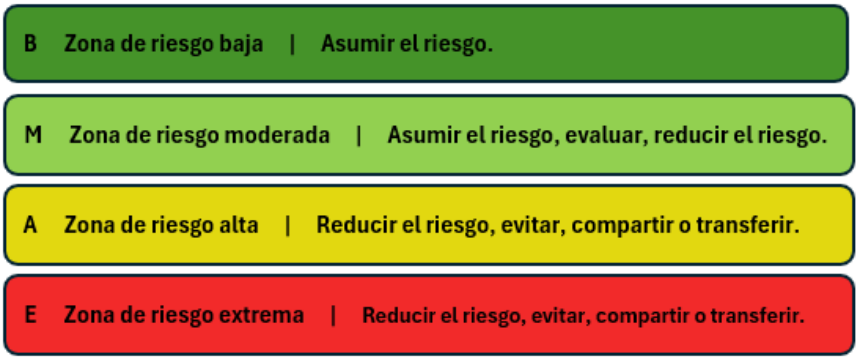
Matriz de Riesgo



Fuente: Elaboración Propia

Figura 5

Zona de Riesgo y guía para asumir incidentes



Fuente: Elaboración Propia

16.1.5 Respuesta a incidentes de seguridad de la información

Control: Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.

Guía de implementación: Los incidentes de seguridad de la información deben ser atendidos por un punto de contacto designado y otras personas relevantes de la organización o partes externas (ver 16.1.1). La respuesta debe incluir lo siguiente:

a) Recopilar evidencia tan pronto como sea posible después de la ocurrencia;
b) Realizar análisis forense de seguridad de la información, según sea necesario (ver 16.1.7);
c) Escalar, según sea necesario;
d) Asegurarse de que todas las actividades de respuesta involucradas estén debidamente registradas para análisis posterior;

e) Comunicar la existencia del incidente de seguridad de la información o cualquier detalle relevante del mismo a otras personas u organizaciones internas y externas que necesiten saberlo;
f) Tratar las debilidades de seguridad de la información encontradas que causen o contribuyan al incidente;
g) Una vez que el incidente haya sido atendido con éxito, cerrarlo y registrarlo formalmente.

Debe realizarse un análisis posterior al incidente, según sea necesario, para identificar la fuente del incidente.

Otra información: El primer objetivo de la respuesta a incidentes es reanudar el 'nivel de seguridad normal' y luego iniciar la recuperación necesaria.

16.1.6 Aprendizaje a partir de incidentes de seguridad de la información

Control: El conocimiento obtenido del análisis y resolución de incidentes de seguridad de la información debe utilizarse para reducir la probabilidad o el impacto de futuros incidentes.

Guía de implementación: Deben existir mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información. La información obtenida de la evaluación de incidentes de seguridad de la información debe usarse para identificar incidentes recurrentes o de alto impacto.

Otra información: La evaluación de los incidentes de seguridad de la información puede indicar la necesidad de controles mejorados o adicionales para limitar la frecuencia, el daño y el costo de futuras ocurrencias, o para ser considerados en el proceso de revisión de la política de seguridad.

Con el debido cuidado de los aspectos de confidencialidad, anécdotas de incidentes reales de seguridad de la información pueden utilizarse en la capacitación de concienciación de los usuarios, como ejemplos de lo que podría suceder, cómo responder a tales incidentes y cómo evitarlos en el futuro.

16.1.7 Recolección de evidencia

Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

Guía de implementación: Se deben desarrollar y seguir procedimientos internos cuando se trate de evidencia para fines disciplinarios y legales.

En general, estos procedimientos para la evidencia deben proporcionar procesos de identificación, recolección, adquisición y preservación de evidencia de acuerdo con diferentes tipos de medios, dispositivos y estados de los dispositivos, por ejemplo, encendidos o apagados. Los procedimientos deben tener en cuenta:

a) Cadena de custodia;
b) Seguridad de la evidencia;
c) Seguridad del personal;
d) Roles y responsabilidades del personal involucrado;
e) Competencia del personal;
f) Documentación;
g) Información previa.

Donde sea posible, se debe buscar la certificación u otros medios relevantes de calificación del personal y las herramientas, para fortalecer el valor de la evidencia preservada.

Otra información:

- La identificación es el proceso que implica la búsqueda, reconocimiento y documentación de evidencia potencial.
- La recolección es el proceso de reunir los elementos físicos que pueden contener evidencia potencial.
- La adquisición es el proceso de crear una copia de datos dentro de un conjunto definido.

- La preservación es el proceso para mantener y salvaguardar la integridad y condición original de la evidencia potencial.

ISO/IEC 27037 proporciona pautas para la identificación, recolección, adquisición y preservación de evidencia digital.

Pasos de Implementación

Identificación de Incidentes

Definición de Incidente de Seguridad

- Un incidente de seguridad es cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de la información.
- Referencia: ISO/IEC 27001, A.16.1.1 - "Gestión de Incidentes de Seguridad de la Información".

Canales de Reporte

- Establecer múltiples canales claros y accesibles para que los empleados reporten incidentes de seguridad, tales como:
    - Un correo electrónico dedicado.
    - Una línea directa telefónica.
    - Un portal web interno para reportes de incidentes.
- Asegurarse de que todos los empleados estén informados sobre estos canales y se les haya capacitado en su uso.
- Referencia: ISO/IEC 27001, A.16.1.2 - "Reporte de Incidentes de Seguridad".

Registro de Incidentes:

- Utilizar un sistema de gestión de incidentes (SGI) para registrar todos los eventos reportados.
- El SGI debe incluir:
    - Fecha y hora del incidente.
    - Descripción del incidente.
    - Identidad del reportante.
    - Impacto percibido.
    - Acciones tomadas.
- Asegurarse de que todos los incidentes se registren de manera oportuna y completa.

- Referencia: ISO/IEC 27001, A.16.1.3 - "Registro de Incidentes de Seguridad".

Respuesta a Incidentes

Evaluación Inicial

- Evaluar la naturaleza y el alcance del incidente inmediatamente después de su reporte.
- Determinar si el incidente es real o un falso positivo.
- Documentar los resultados de la evaluación inicial.
- Referencia: ISO/IEC 27001, A.16.1.4 "Valoración de eventos de seguridad de la información y toma de decisiones".

Clasificación del Incidente

- Clasificar el incidente según su severidad y el impacto potencial en la organización.
- Las categorías pueden incluir:
    - Incidente menor.
    - Incidente moderado.
    - Incidente crítico.

- Utilizar una matriz de impacto y probabilidad para ayudar en la clasificación, misma compartida en la sección anterior.

Asignación de Recursos

- Designar un equipo de respuesta apropiado según la clasificación del incidente.
- Asegurarse de que el equipo tenga las competencias y recursos necesarios para manejar el incidente de manera eficaz.
- Referencia: ISO/IEC 27001, A.16.1.1 "Responsabilidades y procedimientos".

Mitigación de Incidentes

Contención Inmediata

Implementar medidas inmediatas para contener el incidente y prevenir una mayor propagación.

- Ejemplos de medidas de contención incluyen:
    - Desconectar sistemas afectados de la red.
    - Bloquear direcciones IP sospechosas.
- Documentar todas las acciones de contención realizadas.
- Referencia: ISO/IEC 27001, A.16.1.5 " Respuesta a los incidentes de seguridad".

Erradicación

- Identificar y eliminar la causa raíz del incidente.
- Esto puede incluir:
    - Eliminar malware.
    - Corregir vulnerabilidades de software.
- Asegurarse de que la erradicación sea completa antes de proceder con la recuperación.

Recuperación

- Restaurar los sistemas afectados a su estado operativo normal.
- Verificar que todos los sistemas restaurados funcionen correctamente y que no haya signos de reinfección.
- Documentar el proceso de recuperación y cualquier problema encontrado.

Revisión y Mejora

Análisis Post-Incidente

- Realizar un análisis detallado del incidente para identificar lecciones aprendidas.
- Incluir en el análisis:
    - Qué causó el incidente.
    - Cómo se gestionó el incidente.
    - Qué se podría haber hecho mejor.

- Documentar los resultados y compartirlos con el equipo relevante.
- Referencia: ISO/IEC 27001, A.16.1.6 "Aprendizaje de los incidentes de seguridad de la información".

Actualización de Políticas y Procedimientos

- Revisar y actualizar las políticas y procedimientos de seguridad basándose en las lecciones aprendidas del incidente.
- Asegurarse de que los cambios se comuniquen y se implementen de manera efectiva en toda la organización.
- Capacitar al personal según las nuevas políticas y procedimientos.

Auditorías Internas

Planificación de Auditorías

Frecuencia de Auditorías

- Programar auditorías internas al menos una vez al año.
- Determinar la frecuencia adicional basada en factores de riesgo y cambios significativos en el SGSI.

Alcance de las Auditorías

- Definir el alcance de cada auditoría para cubrir todos los aspectos críticos del SGSI.
- Incluir todos los sistemas, procesos y áreas de la organización que manejen información sensible.

Equipo de Auditoría

- Designar un equipo de auditoría independiente y competente.
- Asegurarse de que los auditores tengan las habilidades y conocimientos necesarios para realizar la auditoría de manera efectiva.
- Evitar conflictos de interés dentro del equipo de auditoría.

Ejecución de Auditorías

Recolección de Información

- Recopilar documentación relevante, como políticas de seguridad, procedimientos operativos y registros de cumplimiento.
- Utilizar listas de verificación y herramientas de auditoría para garantizar una recolección de información completa.

Entrevistas y Observación

- Realizar entrevistas con el personal clave y observar los procedimientos en acción.
- Documentar las observaciones y los comentarios de las entrevistas.

Evaluación Técnica

- Utilizar herramientas de auditoría para escanear sistemas y redes en busca de vulnerabilidades y revisar configuraciones de seguridad.
- Realizar pruebas de penetración y análisis de vulnerabilidades según sea necesario.

Documentación y Seguimiento

Informe de Auditoría

- Elaborar un informe detallado documentando los hallazgos, incluyendo áreas de incumplimiento, vulnerabilidades y riesgos identificados.
- Presentar el informe a la alta dirección para su revisión.

Revisión del Informe

- Revisar el informe con los gerentes y el equipo de seguridad de la información, validar los hallazgos y obtener acuerdos sobre las acciones correctivas.
- No conformidad y acciones correctivas:

    - Reaccionar ante la no conformidad
    - Evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir, ni ocurra en otra parte
    - Implementar cualquier acción necesaria
    - Revisar la eficacia de las acciones correctivas llevadas a cabo
    - Si es necesario, hacer cambios al sistema de gestión de la seguridad de la información
- Asegurarse de que todos los comentarios y decisiones se documenten adecuadamente.

Plan de Acción

- Desarrollar un plan de acción para abordar los hallazgos de la auditoría, asignar responsabilidades y establecer plazos para la implementación de las medidas correctivas.
- Monitorear el progreso del plan de acción y ajustar según sea necesario.

Seguimiento

- Realizar seguimientos periódicos para asegurar que las acciones correctivas se implementen de manera efectiva y documentar los progresos.
- Verificar la efectividad de las acciones correctivas y realizar ajustes si es necesario.

APÉNDICE F

Programa de Formación y Concienciación en Seguridad de la Información

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA INFORMÁTICA

PROGRAMACIÓN DE FORMACIÓN Y CONCIENCIACIÓN EN SEGURIDAD DE LA INFORMACIÓN

MELANNIE ANGÉLICA MORA CORRALES

JULIO, 2024

CONTENIDOS

INTRODUCCIÓN

La seguridad de la información es fundamental para salvaguardar los activos de información de cualquier organización, incluyendo datos confidenciales, propiedad intelectual y la integridad de los sistemas. La protección eficaz de estos activos no solo asegura la continuidad del negocio, sino que también fortalece la confianza de los clientes y cumple con las obligaciones legales y regulatorias.

Este manual ofrece una guía para desarrollar un programa de formación y concienciación en seguridad de la información dirigido a todos los empleados de la organización. Basado en los requisitos de la norma ISO/IEC 27001, el programa está diseñado para garantizar que el personal esté completamente capacitado y consciente de las políticas de seguridad vigentes. A través de esta capacitación, los empleados adquirirán conocimientos sobre las mejores prácticas en seguridad, identificarán y mitigarán amenazas potenciales, y responderán adecuadamente a incidentes de seguridad.

El programa no solo abarca aspectos técnicos, sino que también se enfoca en la creación de una cultura de seguridad dentro de la organización. La concienciación de los empleados sobre la importancia de la seguridad de la información es esencial para prevenir brechas y garantizar una defensa proactiva contra posibles ataques. Al implementar este programa, la organización demostrará su compromiso con la seguridad de la información y fomentará un entorno donde cada empleado se sienta responsable de la protección de los datos y sistemas.

En resumen, este manual no solo proporciona los fundamentos para la creación de un programa de formación y concienciación en seguridad de la información, sino que también establece una hoja de ruta para mantener y mejorar continuamente la postura de seguridad de la organización, alineada con los estándares internacionales y las mejores prácticas del sector.

Objetivos de la Guía

El objetivo principal del programa de formación y concienciación es asegurar que todos los empleados comprendan la importancia de la seguridad de la información y sepan cómo proteger los datos sensibles de la organización. Los objetivos específicos incluyen:

7. **Concienciación sobre Amenazas y Vulnerabilidades:** Sensibilizar a los empleados sobre las amenazas de seguridad más comunes y cómo pueden afectar a la organización.
8. **Capacitación en el Uso Seguro de Sistemas y Aplicaciones:** Enseñar a los empleados cómo utilizar las herramientas y sistemas de manera segura.
9. **Preparación para Responder a Incidentes de Seguridad:** Entrenar a los empleados para responder eficazmente a incidentes de seguridad.
10. **Evaluación y Certificación de Conocimientos:** Evaluar el conocimiento de los empleados y asegurar que comprenden las políticas de seguridad.

Alcance

El alcance de este programa de formación y concienciación en seguridad de la información cubre todos los aspectos esenciales para garantizar que los empleados de la organización comprendan y apliquen las políticas y prácticas de seguridad de la información. Este programa está dirigido a todos los niveles de personal, desde la alta dirección hasta los empleados operativos, y abarca las siguientes áreas:

1. **Cobertura de Políticas y Procedimientos de Seguridad**
    a. Descripción detallada de las políticas de seguridad de la información de la organización.
    b. Procedimientos para la gestión de datos sensibles y la protección de la infraestructura de TI.
    c. Roles y responsabilidades de cada empleado en la seguridad de la información.
2. **Formación Técnica y Operativa**
    a. Capacitación en el uso seguro de herramientas y sistemas informáticos.
    b. Métodos de autenticación y gestión de contraseñas.
    c. Procedimientos para el manejo seguro de dispositivos móviles y acceso remoto.
3. **Concienciación sobre Amenazas y Vulnerabilidades**
    a. Información sobre las amenazas de seguridad más comunes, como phishing, malware y ataques de ingeniería social.
    b. Estrategias para identificar y mitigar vulnerabilidades en el entorno de trabajo.
4. **Respuesta a Incidentes de Seguridad**
    a. Procedimientos para reportar y gestionar incidentes de seguridad.
    b. Simulacros y ejercicios prácticos para preparar a los empleados en la respuesta efectiva a incidentes.
    c. Comunicación y coordinación con el equipo de seguridad de la información durante un incidente.
5. **Evaluación y Certificación**
    a. Evaluación continua del conocimiento y la comprensión de los empleados sobre las políticas de seguridad.

   b. Certificación de competencias en seguridad de la información para asegurar que los empleados cumplen con los estándares establecidos.

6. **Actualización y Mejora Continua**
   a. Revisión y actualización periódica del contenido de formación para incluir nuevas amenazas y mejores prácticas.
   b. Feedback de los empleados para mejorar el programa y adaptarlo a las necesidades cambiantes de la organización.
7. **Integración con Otros Programas de Seguridad**
   a. Coordinación con otros programas de seguridad y cumplimiento de la organización.
   b. Alineación con los requisitos y normas de seguridad internacionales, incluyendo ISO/IEC 27001.

Políticas y Controles

La norma ISO/IEC 27001 indica los siguientes controles, en los que se basará este manual para su correcta realización y cumplimiento:

ISO/IEC 27001 A.5.1 Directrices de la Dirección en seguridad de la información: El objetivo de este control es el de dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones.

- **5.1.1 Políticas para la seguridad de la información:** *Se debería definir un conjunto de políticas para la seguridad de la información, aprobado por la dirección, publicado y comunicado a los empleados, así como a todas las partes externas relevantes.*
- Alcance: Aplica a todos los empleados, contratistas y terceros que tengan acceso a los activos de información de la organización.

ISO/IEC 27001 A.7.2 Durante la contratación: El objetivo es el de asegurarse de que los empleados y contratistas están en conocimiento y cumplen con sus responsabilidades en seguridad de la información.

- **7.2.2 Concienciación, educación y capacitación en SI:** *Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.*

Objetivo: Fomentar una cultura de seguridad y asegurar que todos los empleados estén informados y preparados.

ISO/IEC 27001 A.8.1 Responsabilidad sobre los activos: El objetivo es identificar los activos en la organización y definir las responsabilidades para una protección adecuada.

- **8.1.3 Uso aceptable de los activos:** *Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.*
- **8.1.4 Devolución de activos:** *Todos los empleados y usuarios de terceras partes deberían devolver todos los activos de la organización que estén en su posesión/responsabilidad,*

una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo.

- Alcance: Todo el personal y cualquier persona que utilice los recursos tecnológicos de la organización.

ISO/IEC 27001 A.9.1 Requisitos de negocio para el control de accesos: El objetivo es controlar los accesos a la información y las instalaciones utilizadas para su procesamiento.

- **9.1.1 Política de control de accesos:** *Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.*
- Alcance: Todos los sistemas de información y recursos tecnológicos.

ISO/IEC 27001 A.9.3 Responsabilidades del usuario: El objetivo es hacer que los usuarios sean responsables de la protección de la información para su identificación.

- **9.3.1 Uso de información confidencial para la autenticación:** *Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación.*
- Alcance: Todos los usuarios que acceden a los sistemas y aplicaciones de la organización.

ISO/IEC 27001 A.14.2 Seguridad en los procesos de desarrollo y soporte: El objetivo de este control es garantizar la seguridad de la información en los entornos de diseño e implementación dentro del ciclo de vida de desarrollo de los sistemas de información.

- **14.2.2 Procedimientos de control de cambios en los sistemas:** *En el ciclo de vida de desarrollo se deberían hacer uso de procedimientos formales de control de cambios.*

Objetivo: Minimizar los riesgos asociados con cambios no autorizados o mal gestionados.

ISO/IEC 27001 A.16.1 Gestión de incidentes de seguridad de la información y mejoras: El objetivo es asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información incluyendo la comunicación de los eventos de seguridad y debilidades.

- **16.1.1 Responsabilidades y procedimientos:** *Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.*
- **16.1.2 Notificación de los eventos de seguridad de la información:** *Los eventos de seguridad de la información se deberían informar lo antes posible utilizando los canales de administración adecuados.*
- **16.1.3 Notificación de puntos débiles de la seguridad:** *Se debería requerir anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la organización.*
- **16.1.5 Respuesta a los incidentes de seguridad:** *Se debería responder ante los incidentes de seguridad de la información en atención a los procedimientos documentados.*
- **16.1.7 Recopilación de evidencias:** *La organización debería definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.*
- Alcance: Todos los incidentes de seguridad que puedan afectar a la organización.

ISO/IEC 27001 A.18.1 Cumplimiento de los requisitos legales y contractuales: El objetivo es evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y/o de cualquier otro requisito de seguridad.

- **18.1.4 Protección de datos y privacidad de la información personal:** *Se debería garantizar la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables que correspondan.*
- Alcance: Todos los datos personales procesados por la organización.

Estructura del Programa

Cobertura de Políticas y Procedimientos de Seguridad

Descripción Detallada de las Políticas de Seguridad de la Información de la Organización

- **Contenido**: Explicación de las políticas clave de la organización relacionadas con la seguridad de la información, incluyendo políticas de control de acceso, gestión de contraseñas, uso aceptable de recursos tecnológicos, gestión de incidentes de seguridad, y protección de datos personales.
- **Frecuencia**: Sesión inicial durante la incorporación y revisión anual.
- **Referencia:** Guía de Configuración Uniforme de Medidas de Seguridad en Dispositivos. (Corrales, 2024)

Procedimientos para la Gestión de Datos Sensibles y la Protección de la Infraestructura de TI

- **Contenido**: Procedimientos específicos para la clasificación y manejo de datos sensibles, medidas de protección física y lógica, y directrices para el acceso seguro a la infraestructura de TI.
- **Frecuencia**: Capacitación inicial y actualizaciones trimestrales.
- **Procedimiento:**
    - Autenticación Multifactor: Implementar autenticación multifactor (MFA) para acceder a sistemas críticos.
    - Políticas de Contraseñas: Establecer y aplicar políticas de contraseñas robustas que incluyan requisitos de longitud, complejidad y periodicidad de cambio.
    - Gestión de Privilegios: Aplicar el principio de privilegios mínimos, otorgando a los usuarios solo los permisos necesarios para realizar sus tareas.
    - Revisión de Accesos: Realizar revisiones periódicas de los permisos de acceso y ajustar según sea necesario para asegurar que sólo el personal autorizado tenga acceso.

Roles y Responsabilidades de Cada Empleado en la Seguridad de la Información

- **Contenido**: Definición de roles y responsabilidades específicos para cada empleado en relación con la seguridad de la información, incluyendo la identificación de responsabilidades individuales y de equipo.
- **Frecuencia**: Capacitación inicial y revisión semestral.
- **Referencia**: Manual de Gestión de Seguridad de la Información. (Corrales, 2024).

Formación Técnica y Operativa

Capacitación en el Uso Seguro de Herramientas y Sistemas Informáticos

- **Contenido**: Instrucciones detalladas sobre el uso seguro de las herramientas y sistemas informáticos utilizados en la organización, incluyendo configuraciones de seguridad y mejores prácticas.
- **Frecuencia**: Capacitación inicial y actualizaciones semestrales.
- **Referencia**: Plan de Migración a Infraestructura de Acceso Remoto y Seguro. (Corrales, 2024)

Métodos de Autenticación y Gestión de Contraseñas

- **Contenido**: Técnicas para la creación y gestión segura de contraseñas, uso de autenticación multifactor, y políticas de renovación de contraseñas.
- **Frecuencia**:
    - Capacitación Inicial: Introducción a la gestión segura de contraseñas y uso de MFA para todos los nuevos empleados.
    - Talleres Trimestrales: Actualización de conocimientos, revisión de políticas y prácticas, y entrenamiento práctico en la creación y gestión segura de contraseñas, y uso de MFA.
- **Procedimiento**:
    - Frecuencia de Cambio: Establecer una política que obligue a los usuarios a cambiar sus contraseñas cada 90 días, por ejemplo.

- Historial de Contraseñas: Implementar una política que impida el uso de las últimas 5 contraseñas utilizadas por el usuario.
- Notificaciones de Cambio: Enviar notificaciones de recordatorio a los usuarios 14 días antes de la fecha límite para el cambio de contraseña.
- Validación de Nuevas Contraseñas: Verificar que las nuevas contraseñas cumplen con los requisitos de seguridad antes de aceptar el cambio.
- Bloqueo de Cuentas: Bloquear automáticamente las cuentas cuya contraseña no se haya renovado en el periodo establecido.
- Proceso de Recuperación: Establecer un proceso seguro para la recuperación de cuentas bloqueadas que incluya la verificación de identidad del usuario.
- Re inicialización de Contraseñas: Permitir la re inicialización de contraseñas caducadas mediante un proceso seguro que pueda incluir MFA.
- Educación Continuada: Incluir en la capacitación periódica información sobre la importancia de cambiar las contraseñas y las consecuencias de no hacerlo.

Procedimientos para el Manejo Seguro de Dispositivos Móviles y Acceso Remoto

- **Contenido**: Directrices para el uso seguro de dispositivos móviles, políticas de BYOD (Bring Your Own Device), y procedimientos seguros para el acceso remoto a la red de la organización.
- **Frecuencia**: Capacitación inicial y revisiones trimestrales.

Guía Paso a Paso para la configuración

- Descargar las aplicaciones de Office:
  - Abra la tienda de aplicaciones de su dispositivo móvil (App Store en iOS o Google Play Store en Android).
  - Busque las aplicaciones de Office que desee instalar, como Outlook, Word, Excel, PowerPoint, etc.
  - Toque en "Instalar" o "Obtener" para descargar e instalar cada aplicación en su dispositivo.

- Abrir la aplicación de Outlook:
    - Abra la aplicación de Outlook en su dispositivo móvil.
    - Si es la primera vez que abre la aplicación, se le pedirá que agregue una cuenta de correo electrónico.
- Agregar una cuenta de correo electrónico en Outlook:
    - Toque en "Comenzar" o "Get Started".
    - Ingrese su dirección de correo electrónico de Microsoft 365 y toque en "Agregar cuenta" o "Add Account".
    - Ingrese la contraseña de su cuenta de correo electrónico y toque en "Iniciar sesión" o "Sign In".
- Configurar la sincronización de correo electrónico:
    - Si se le solicita, configure las opciones de sincronización de su correo electrónico, como la frecuencia de actualización y los elementos a sincronizar (correo, contactos, calendario, etc.).
    - Toque en "Listo" o "Done" para completar la configuración.
- Abrir otras aplicaciones de Office:
    - Abra cada una de las aplicaciones de Office que haya descargado (Word, Excel, PowerPoint, etc.).
    - Inicie sesión con su cuenta de Microsoft 365 en cada aplicación.
- Iniciar sesión en las aplicaciones de Office:
    - En cada aplicación, toque en "Iniciar sesión" o "Sign In".
    - Ingrese su dirección de correo electrónico y contraseña de Microsoft 365.
    - Toque en "Iniciar sesión" o "Sign In" para completar la configuración.
- Configurar el almacenamiento en la nube:
    - En las aplicaciones de Office, puede configurar el acceso a su almacenamiento en la nube de OneDrive o SharePoint.
    - Toque en "Abrir" o "Open" y seleccione "Agregar un lugar" o "Add a place".
    - Seleccione OneDrive o SharePoint y siga las instrucciones para conectar su cuenta.
- Sincronizar archivos y documentos:

    - Asegúrese de que la sincronización de archivos esté habilitada para que pueda acceder a sus documentos desde cualquier dispositivo.
    - Puede abrir, editar y guardar documentos directamente en su almacenamiento en la nube desde las aplicaciones de Office.
- Personalizar las configuraciones de las aplicaciones:
    - En cada aplicación de Office, puede acceder a las configuraciones para personalizar la experiencia de usuario.
    - Toque en el ícono de configuración (generalmente representado por tres puntos o un engranaje) y ajuste las opciones según sus preferencias.
- Explorar las funcionalidades de las aplicaciones:
    - Explore las funcionalidades y características de cada aplicación de Office para aprovechar al máximo sus capacidades.
    - Puede encontrar tutoriales y guías dentro de las aplicaciones o en el sitio web de soporte de Microsoft.
- **Referencia**: Documentación oficial del proveedor. Configurar el correo electrónico y las aplicaciones de Office en un dispositivo móvil. (Microsoft Corporation, 2024)

Concienciación sobre Amenazas y Vulnerabilidades

Información sobre las Amenazas de Seguridad más Comunes

- **Contenido**: Descripción de las amenazas más comunes como phishing, malware, ransomware, y ataques de ingeniería social, incluyendo ejemplos reales y métodos de prevención.
- **Frecuencia**: Sesiones trimestrales y boletines mensuales.

Paso a Paso para Crear un Manual de Formación en Seguridad de la Información

1. Definir el Objetivo del Manual:

- Establezca claramente el objetivo del manual, que es educar a los empleados sobre las amenazas de seguridad de la información y proporcionarles estrategias para minimizar los riesgos.

2. Identificar las Amenazas y Vulnerabilidades Más Comunes:
   - Haga una lista de las amenazas y vulnerabilidades más comunes que su organización enfrenta. Algunas de las más frecuentes incluyen:
     - Phishing
     - Malware
     - Ransomware
     - Ingeniería social
     - Robo de identidad
     - Accesos no autorizados
     - Vulnerabilidades en el software
3. Desarrollar una Sección Introductoria:
   - Proporcione una introducción general sobre la importancia de la seguridad de la información.
   - Explique cómo las amenazas pueden afectar a la organización y a los empleados.
4. Describir Cada Amenaza y Vulnerabilidad:
   - Para cada amenaza identificada, incluya una descripción detallada que explique:
     - Qué es la amenaza o vulnerabilidad.
     - Cómo se manifiesta.
     - Ejemplos reales (si es posible).
5. Incluir Consejos para Reconocer Amenazas:
   - Ofrezca pautas específicas para ayudar a los empleados a reconocer señales de amenazas, como:
     - **Phishing**: Correos electrónicos con enlaces sospechosos, remitentes desconocidos, urgencia inusual.
     - **Malware**: Descargas de fuentes no confiables, comportamientos inusuales del sistema.

        - **Ingeniería social**: Solicitudes de información confidencial por parte de personas desconocidas o no autorizadas.
6. Proporcionar Estrategias para Minimizar Riesgos:
    - Para cada amenaza, describa las mejores prácticas y estrategias para minimizar los riesgos. Esto puede incluir:
        - Uso de software antivirus y antimalware actualizado.
        - Formación continua sobre la identificación de correos electrónicos de phishing.
        - Contraseñas seguras y uso de autenticación multifactor.
        - Políticas de acceso estrictas y control de privilegios.
        - Actualización regular del software y los sistemas operativos.
7. Incluir Procedimientos de Respuesta a Incidentes:
    - Describa los pasos que deben seguir los empleados en caso de detectar una amenaza o si creen que han sido comprometidos:
        - Reportar inmediatamente al equipo de TI o al departamento de seguridad.
        - No interactuar con correos electrónicos o archivos sospechosos.
        - Seguir los protocolos de respuesta a incidentes establecidos por la organización.
8. Crear Ejercicios y Evaluaciones:
    - Incluya ejercicios prácticos, cuestionarios y escenarios de simulación para reforzar el aprendizaje.
    - Evaluaciones periódicas para medir el conocimiento y la preparación de los empleados.
9. Añadir Recursos Adicionales:
    - Proporcione una lista de recursos adicionales donde los empleados puedan obtener más información, como:
        - Enlaces a artículos y tutoriales en línea.
        - Contacto del equipo de seguridad de la información.
        - Acceso a la política de seguridad de la organización.
10. Revisar y Actualizar el Manual Regularmente:

- Asegúrese de que el manual se revise y actualice regularmente para reflejar las nuevas amenazas y las mejores prácticas más recientes.
- Fomente la retroalimentación de los empleados para mejorar continuamente el contenido del manual.

Estructura Sugerida del Manual

1. Introducción
    - Importancia de la seguridad de la información
    - Objetivos del manual
2. Amenazas y Vulnerabilidades Comunes
    - Descripción de cada amenaza
    - Ejemplos y casos reales
3. Reconocimiento de Amenazas
    - Señales y síntomas de amenazas
4. Minimización de Riesgos
    - Estrategias y mejores prácticas
5. Respuesta a Incidentes
    - Procedimientos y protocolos
6. Ejercicios y Evaluaciones
    - Cuestionarios y simulaciones
7. Recursos Adicionales
    - Enlaces y contactos útiles
8. Revisión y Actualización
    - Procedimiento para la actualización del manual

Este enfoque le ayudará a crear un manual integral y práctico que educará a sus empleados sobre cómo protegerse a sí mismos y a la organización contra las amenazas de seguridad de la información.

- **Referencia**: Se puede basar el contenido en una referencia confiable tal como lo es 6 Principales Amenazas Ciberseguridad. (CheckPoint, 2024)

Estrategias para Identificar y Mitigar Vulnerabilidades en el Entorno de Trabajo

- **Contenido**: Técnicas para identificar posibles vulnerabilidades en el entorno de trabajo y medidas correctivas para mitigarlas.
- **Frecuencia**: Talleres semestrales y ejercicios prácticos anuales.
- **Procedimientos**:
    - Software de Seguridad: Instalar y actualizar regularmente software antivirus, antimalware y firewall en todos los sistemas.
    - Actualizaciones y Parches: Mantener todos los sistemas operativos y aplicaciones actualizados con los últimos parches de seguridad.
    - Monitoreo de Sistemas: Implementar sistemas de monitoreo y detección de intrusiones (IDS/IPS) para identificar y responder a actividades sospechosas.
    - Educación de Usuarios: Capacitar a los empleados sobre las mejores prácticas de seguridad, incluyendo cómo reconocer y evitar ataques de phishing y otras amenazas.

Respuesta a Incidentes de Seguridad

Procedimientos para Reportar y Gestionar Incidentes de Seguridad

- **Contenido**: Instrucciones claras sobre cómo reportar incidentes de seguridad, flujo de trabajo de gestión de incidentes, y roles y responsabilidades durante un incidente.
- **Frecuencia**: Capacitación inicial, revisiones semestrales y ejercicios prácticos anuales.
- **Referencia**: Manual de Gestión de Incidentes y Auditorías Internas. (Corrales, 2024)

Simulacros y Ejercicios Prácticos para Preparar a los Empleados en la Respuesta Efectiva a Incidentes

- **Contenido**: Simulacros de incidentes y ejercicios de mesa para ensayar la respuesta a diferentes tipos de incidentes de seguridad.
- **Frecuencia**: Ejercicios trimestrales y simulacros anuales.

Comunicación y Coordinación con el Equipo de Seguridad de la Información Durante un Incidente

- **Contenido**: Procedimientos de comunicación interna y externa durante un incidente de seguridad, coordinación con el equipo de seguridad y otros departamentos.
- **Frecuencia**: Capacitación inicial y revisiones semestrales.

Evaluación y Certificación

Evaluación Continua del Conocimiento y la Comprensión de los Empleados sobre las Políticas de Seguridad

- **Contenido**: Evaluaciones periódicas a través de cuestionarios, encuestas y pruebas para medir el conocimiento y la comprensión de los empleados sobre las políticas de seguridad.
- **Frecuencia**: Evaluaciones semestrales.

Actualización y Mejora Continua

Revisión y Actualización Periódica del Contenido de Formación

- **Contenido**: Evaluación y actualización del material de formación para incluir nuevas amenazas, tecnologías y mejores prácticas en seguridad de la información.
- **Frecuencia** Evaluación del contenido de formación cada seis meses e incorporación de nuevas amenazas, tecnologías y mejores prácticas anualmente.
- **Procedimientos**:
    - Análisis de Incidentes: Utilizar datos de incidentes de seguridad recientes para identificar temas que deben ser abordados o reforzados en el contenido de formación.

- Monitoreo de Amenazas: Mantenerse informado sobre nuevas amenazas y vulnerabilidades mediante la suscripción a boletines de seguridad y la participación en foros y conferencias de seguridad.
- Integración de Nuevas Tecnologías: Actualizar el contenido de formación para incluir nuevas tecnologías y herramientas de seguridad, como soluciones avanzadas de autenticación, cifrado y análisis de seguridad.

Feedback de los Empleados para Mejorar el Programa

- **Contenido**: Recopilación de feedback de los empleados a través de encuestas y sesiones de retroalimentación para identificar áreas de mejora en el programa de formación.
- **Frecuencia**: Encuestas trimestrales y sesiones de retroalimentación semestrales.
- **Procedimientos**:
  - Diseño de Encuestas: Crear encuestas breves y específicas que evalúen la efectividad y relevancia del contenido de formación.
  - Distribución: Enviar las encuestas a todos los empleados trimestralmente.
  - Programación de Sesiones: Organizar sesiones de retroalimentación con grupos representativos de empleados cada seis meses.

Integración con Otros Programas de Seguridad

Alineación con los Requisitos y Normas de Seguridad Internacionales

- **Contenido**: Asegurar que el programa cumple con los estándares internacionales de seguridad, incluyendo ISO/IEC 27001, y otras normativas relevantes.
- **Frecuencia**: Auditorías anuales y revisiones semestrales.
- **Procedimiento:**
  - Programación de Reuniones: Establecer reuniones regulares (mensuales o trimestrales) entre los responsables de los distintos programas de seguridad.
  - Intercambio de Información: Compartir información relevante sobre amenazas, incidentes y mejores prácticas.

- Sinergia de Estrategias: Identificar oportunidades para alinear estrategias y acciones entre los programas de seguridad para maximizar la protección de los activos de información.
- Plan de Acción Conjunto: Desarrollar y actualizar un plan de acción conjunto para abordar amenazas y mejorar la postura de seguridad de la organización.

REFERENCIAS

CheckPoint. (2024). *Top 6 Cybersecurity Threats*. Retrieved from CheckPoint: https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-cybersecurity/top-6-cybersecurity-threats/

Corrales, M. M. (2024). *Guía de Configuración Uniforme de Medidas de Seguridad en Dispositivos.* San Jose.

Corrales, M. M. (2024). *Manual de Gestión de Incidentes y Auditorías Internas.* San Jose.

Corrales, M. M. (2024). *Manual de Gestión de Seguridad de la Información.* San José.

Corrales, M. M. (2024). *Plan de Migración a Infraestructura de Acceso Remoto y Seguro.* San Jose.

Microsoft Corporation. (2024). *Configurar el correo electrónico y las aplicaciones de Office en un dispositivo móvil*. Retrieved from Microsoft Support: https://support.microsoft.com/es-es/office/configurar-el-correo-electr%C3%B3nico-y-las-aplicaciones-de-office-en-un-dispositivo-m%C3%B3vil-7dabb6cb-0046-40b6-81fe-767e0b1f014f