MAESTRÍA EN CIBERSEGURIDAD

PROYECTO DE TITULACIÓN

Modalidad Proyecto de Investigación y Desarrollo

Fortalecimiento del Desarrollo E Implementación de Políticas de Seguridad y Capacitación Continua de Nuestros Empleados

Autor: Katherine Estefanía Ledesma Pazmiño

Guía: Roque Jacinto Hernández Bustos

Presentando como parte de los requisitos para el título de magister en ciberseguridad.

Guayaquil, 18 de Marzo del 2024

LEDESMA PAZMIÑO, KATHERINE ESTEFANÍA en calidad de autor y titular del trabajo de titulación "Implementación de Medidas de Seguridad en Una Empresa Mediana" para optar por la **Maestría en Ciberseguridad**, autorizo a la Universidad Casa Grande para que realice la digitalización y publicación de este trabajo de titulación en su Repositorio Digital de acceso abierto, con fines estrictamente académicos, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Asimismo, autorizo a la Universidad Casa Grande a reproducir, distribuir, comunicar y poner a disposición del público mi documento de trabajo de titulación en formato físico o digital y en cualquier medio sin modificar su contenido, sin perjuicio del reconocimiento que deba hacer la Universidad sobre la autoría de dichos trabajos.

LEDESMA PAZMIÑO, KATHERINE ESTEFANÍA
1206870378

PROPUESTA DE CLÁUSULA DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJOS DE TITULACIÓN

Yo, LEDESMA PAZMIÑO, KATHERINE ESTEFANÍA, autor del trabajo de titulación "Implementación de Medidas de Seguridad en Una Empresa Mediana", certifico que el ensayo reflexivo es una creación de mi autoría, por lo que sus contenidos son originales, de exclusiva responsabilidad de su autor y no infringen derechos de autor de terceras personas. Con lo cual, exonero a la Universidad Casa Grande de reclamos o acciones legales.

Ing. Katherine L

LEDESMA PAZMIÑO, KATHERINE ESTEFANÍA
1206870378

INTRODUCIÒN

En un mundo cada vez más interconectado y dependiente de la tecnología, la seguridad de la información se ha convertido en un aspecto fundamental para cualquier empresa. Los avances tecnológicos han proporcionado innumerables beneficios, pero también han traído consigo nuevas amenazas y vulnerabilidades que pueden comprometer la integridad, confidencialidad y disponibilidad de los datos empresariales. En este contexto, el desarrollo e implementación de políticas de seguridad robustas y la capacitación continua de los empleados se vuelven imperativas para proteger los activos digitales de una organización. Las políticas de seguridad establecen las normas, procedimientos y controles necesarios para mitigar riesgos y garantizar un entorno seguro, mientras que la capacitación proporciona a los empleados los conocimientos y habilidades necesarios para identificar, prevenir y responder a posibles amenazas cibernéticas.

Es importante reconocer que la seguridad en la era digital es responsabilidad de todos en la organización. Cada empleado juega un papel crucial en la protección de la información sensible y en la prevención de ataques cibernéticos. Por lo tanto, fomentar una cultura de seguridad y promover la conciencia de los riesgos entre el personal son aspectos fundamentales para fortalecer la postura de seguridad de la empresa. En esta propuesta, exploraremos la importancia de desarrollar políticas de seguridad sólidas, así como la necesidad de capacitar y educar a los empleados de manera continua para enfrentar los desafíos de seguridad en la era digital. Además, discutiremos cómo estas medidas pueden ayudar a proteger los activos digitales de la empresa y a mantener la confianza de los clientes y socios comerciales.

RESUMEN

El presente trabajo de titulación tiene como objetivo principal el desarrollo e implementación de las políticas de seguridad en una organización. Para ello, se realizó una evaluación inicial en donde se identificó los riesgos de no contar con políticas de seguridad en las cuales categorizamos como criticas el acceso de privilegios de accesos a los servicios y componentes críticos en su sistema, encontramos contraseñas débiles, procesos incompletos entre otros factores.

A partir de esta evaluación, se sugirió y se impulsó la implementación de una solución desarrollar políticas de seguridad ajusta a las necesidades y características de la organización y se procedió a su implementación Se realizaron pruebas y verificación para garantizar el correcto funcionamiento del sistema y se actualizaron los procesos actuales de accesos en función al tipo de acceso y flujo de aprobación para el uso de las cuentas privilegiadas en la empresa, salvaguardando la triada de la seguridad de la información: confidencialidad, integridad y disponibilidad.

Los resultados obtenidos indican que la implementación del de las políticas de seguridad fortalecerá la seguridad de la información en la organización, al permitir un mayor control y monitoreo.

OBJETIVO

Fortalecer la seguridad de la empresa mediante el desarrollo e implementación de políticas de seguridad robustas y la capacitación continua de los empleados, con el fin de reducir el riesgo de incidentes de seguridad cibernética y proteger los activos digitales de la organización contra amenazas internas y externas.

DESARROLLO

GERENCIA, OPERACIÓN Y PLANIFICACIÓN DE LA CIBERSEGURIDAD

Fue primordial en el proceso de aprendizaje de esta maestría, ya que me proporcionó las bases para poder iniciar una implementación de unas políticas de seguridad. Durante este módulo, se exploraron las herramientas necesarias para establecer políticas de seguridad de la información, abarcando desde el control interno hasta los parámetros que deben regir en la organización. Esta formación es esencial para garantizar la protección de los datos y la continuidad de los servicios que ofrecen.

El libro Ciberseguridad: Protegiendo tus datos en un mundo digital aborda diversos aspectos relacionados con la gestión estratégica, operativa y planificación de la ciberseguridad en el contexto empresarial. Proporciona información sobre cómo desarrollar políticas de seguridad efectivas, gestionar incidentes de seguridad, implementar controles de acceso y planificar la respuesta ante amenazas cibernéticas. Es una lectura útil tanto para gerentes como para profesionales de TI que buscan fortalecer la seguridad de sus organizaciones en un entorno digital cada vez más complejo y dinámico. (Adam McNeil,2020)

En este módulo, se adquirió conocimientos fundamentales relacionados con los controles internos y los procesos necesarios para administrar, dirigir y diseñar un plan estratégico de Ciberseguridad en la organización anteriormente mencionada. A grandes

rasgos, se abordó el desarrollo de políticas de seguridad a corto, mediano y largo plazo. Esto incluyó la definición de parámetros esenciales como la planificación, identificación, medición, control/mitigación, monitoreo/revisión y comunicación/consulta, de esta manera, se proyectó el desarrollo de las políticas de ciberseguridad.

EL MÓDULO DE TECNOLOGÍA, MODELOS Y TÉCNICAS DE CIBERSEGURIDAD

Es fundamental en el proceso de aprendizaje sobre ciberseguridad. No se trata solo de proteger la información almacenada en los repositorios digitales, sino también de comprender las redes y sus protocolos de comunicación, para garantizar una comunicación eficiente en las redes alámbricas e inalámbricas, es crucial reducir la interferencia y garantizar una conexión segura y fiable, la calidad de los conectores y paneles de control, así como las configuraciones de los switches y routers, son pasos fundamentales para fortalecer la ciberseguridad y proteger la integridad de la infraestructura de red.

En este módulo se profundiza el funcionamiento de los protocolos UTP y UDP, así como en su vulnerabilidad ante ataques como el sniffing, el vandalismo, la inserción de HUBS y el envenenamiento ARP, estos ataques pueden llegar a surgir si no se toman las precauciones adecuadas al configurar los switches, por lo tanto, es importante cerrar los puertos de estos equipos, de manera apropiada para evitar intrusiones en la red por parte de personas externas que buscan sustraer información confidencial.

El libro Ciberseguridad: Técnicas, tecnologías y buenas prácticas para garantizar la seguridad en la red proporciona una visión detallada de las técnicas y tecnologías utilizadas en ciberseguridad, así como de los modelos y buenas prácticas recomendadas

para proteger los sistemas de información contra amenazas cibernéticas. Cubre una amplia gama de temas, desde la criptografía hasta la detección de intrusiones, pasando por la gestión de riesgos y la seguridad en redes, ofreciendo una perspectiva integral sobre cómo abordar los desafíos de seguridad en entornos digitales. (José María Foces Morán, 2019).

Durante el levantamiento de información, se observó contraseñas débiles, usuarios con pocos conocimientos sobre la seguridad de sus equipos, procesos incompletos, no contar con un plan de mitigación ante cualquier riesgo.

En respuesta a estas observaciones, se ha realizado la documentación de políticas de seguridad y capacitación para los usuarios.

ESTRATEGIAS Y POLÍTICAS MULTILATERALES PARA LA CIBERSEGURIDAD

Esencial el aprendizaje en Ciberseguridad, ya que permitió revisar bases sobre las Políticas Nacionales en Ciberseguridad, como ha ido evolucionando en el medio y el alcance que en la actualidad tiene la seguridad de la información, las políticas creadas por el Ministerio de telecomunicaciones en el manejo de la seguridad de la información, profundizando también sobre el Sistema de Gestión de Seguridad de la Información (SGSI), por qué esta deben se implementadas en las diferentes empresas, para salvaguardar la seguridad de la información y sobre todo lo más relevante que es Alcanzar una Certificación ISO 27001, respetando las leyes y normativas vigentes como la Ley Orgánica de Protección de Datos y su reglamento que busca proteger a los datos e información de los ciudadanos contra el abuso, Código Orgánico Integral Penal (COIP).

El aprendizaje de este módulo permitió la elaboración de un Plan Estratégico de Seguridad Informática (PESI), este plan, abarca las responsabilidades y políticas necesarias para garantizar la seguridad cibernética en la organización protegiendo la seguridad de la información estableciendo restricciones, ya que en la actualidad no existen, por otro lado, cabe mencionar la realización de charlas en ciberseguridad permite hacer hincapié sobre el Fishing y lo que abarca este.

El libro The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations analiza las complejidades de las estrategias y políticas multilaterales en el ámbito de la ciberseguridad, centrándose en las relaciones entre naciones y los dilemas éticos y políticos que surgen en el contexto de la ciberseguridad. Explora cómo las acciones ofensivas y defensivas en el ciberespacio pueden afectar las relaciones internacionales y la estabilidad geopolítica, así como los desafíos de establecer normas y acuerdos internacionales en este campo en constante evolución. Es una lectura esencial para comprender las dinámicas y los debates en torno a las estrategias y políticas multilaterales para la ciberseguridad. (Ben Buchanan,2017)

Con la elaboración del Plan de Acción se realizará la implementación de las políticas de seguridad, capacitación al personal se podrá realizar análisis de riesgo, estableciendo normas, políticas y procedimientos, seguridad a los activos físicos y lógicos, evaluación de riesgos, controles de seguridad, y sobre todo auditorías y revisiones.

HACKING ÉTICO Y ANÁLISIS DEL CIBERATAQUE

Permite conocer sobre las técnicas de hacking aplicadas a las redes, direccionando la exploración de la vulnerabilidad inherente de las redes si no se cuenta con un buen firewall, sin duda, lo más fascinante es la realización de pruebas de penetración utilizando Kali Linux en una red determinada, estas pruebas permiten identificar posibles intrusos.

El libro Hacking Ético: Cómo hackear profesionalmente en 21 días o menos proporciona una introducción completa al mundo del hacking ético, desde los fundamentos básicos hasta técnicas avanzadas de penetración y análisis de vulnerabilidades. Además de explorar herramientas y metodologías utilizadas por los hackers éticos, también aborda conceptos éticos y legales relacionados con la seguridad informática. Es una lectura útil tanto para principiantes como para profesionales de seguridad que deseen mejorar sus habilidades en el campo del hacking ético y la defensa contra ciberataques. (Daniel M. Filipe,2020)

En el fortalecimiento del desarrollo e implementación de políticas de seguridad y la capacitación continua de los empleados puede ser altamente beneficioso para mejorar la postura de seguridad de la empresa permitiendo detallar los aspectos claves:

- **Capacitación en Hacking Ético**: Ofrecer sesiones de formación sobre técnicas y metodologías de hacking ético para que los empleados comprendan cómo piensan los hackers malintencionados y puedan identificar posibles vulnerabilidades en los sistemas de la empresa.
- **Simulacros de Ciberataques**: Organizar ejercicios prácticos de simulación de ciberataques para que los empleados adquieran experiencia práctica en la detección, respuesta y mitigación de amenazas cibernéticas, utilizando técnicas de hacking ético para comprender cómo operan los atacantes.
- **Análisis de Incidentes de Seguridad**: Formar a los empleados en el análisis de incidentes de seguridad para que puedan investigar y comprender la naturaleza de los ciberataques que afectan a la empresa, identificar el alcance del incidente y desarrollar respuestas efectivas.
- **Desarrollo de Políticas de Seguridad Basadas en Amenazas**: Utilizar los conocimientos adquiridos en hacking ético y análisis de ciberataques para informar el desarrollo de políticas de seguridad que aborden las amenazas específicas que enfrenta la empresa, asegurando una protección proactiva contra posibles ataques.

- **Fomento de la Conciencia de Seguridad**: Integrar lecciones de hacking ético y análisis de ciberataques en programas de concienciación de seguridad para sensibilizar a los empleados sobre las tácticas utilizadas por los ciberdelincuentes y promover buenas prácticas de seguridad.
- **Evaluaciones de Vulnerabilidades Controladas**: Realizar evaluaciones de vulnerabilidades controladas internamente, donde se permita a los empleados aplicar técnicas de hacking ético para identificar debilidades en la infraestructura y aplicaciones de la empresa, con el objetivo de mejorar la seguridad de manera proactiva.

- **Certificaciones y Formación Continua**: Apoyar a los empleados interesados en obtener certificaciones en hacking ético y ciberseguridad, y proporcionar oportunidades de formación continua para mantenerse actualizados sobre las últimas técnicas y tendencias en el ámbito de la seguridad cibernética.

El desarrollo e implementación de políticas de seguridad y la capacitación continua de los empleados puede mejorar significativamente la capacidad de la empresa para proteger sus activos digitales y responder eficazmente a las amenazas cibernéticas en constante evolución.

CONTINUIDAD DEL NEGOCIO

En el fortalecimiento del desarrollo e implementación de políticas de seguridad y la capacitación continua de los empleados es fundamental para garantizar la resiliencia de la empresa frente a posibles interrupciones o desastres. permitiendo detallar los aspectos claves:

- **Incorporación de Planes de Continuidad del Negocio en las Políticas de Seguridad**: Desarrollar políticas de seguridad que incluyan planes de

continuidad del negocio como parte integral de la estrategia de protección de activos digitales. Estos planes deben abordar cómo mantener las operaciones críticas durante y después de un incidente de seguridad.

- **Capacitación en Procedimientos de Continuidad del Negocio**: Proporcionar capacitación regular a los empleados sobre los procedimientos y protocolos de continuidad del negocio, incluyendo cómo identificar y responder a situaciones de crisis, y cómo mantener la operatividad de los sistemas y servicios esenciales.
- **Simulacros de Continuidad del Negocio**: Realizar ejercicios periódicos de simulación de situaciones de crisis para que los empleados practiquen la implementación de los planes de continuidad del negocio en escenarios realistas. Esto ayuda a mejorar la preparación y la capacidad de respuesta del personal ante emergencias.
- **Evaluación de Riesgos y Vulnerabilidades**: Integrar la continuidad del negocio en los procesos de evaluación de riesgos y vulnerabilidades de seguridad, identificando las amenazas que podrían afectar la continuidad de las operaciones y desarrollando estrategias para mitigar estos riesgos.
- **Respaldo y Recuperación de Datos**: Garantizar que existan procedimientos sólidos de respaldo y recuperación de datos como parte de los planes de continuidad del negocio, asegurando la disponibilidad y la integridad de la información crítica en caso de un incidente de seguridad.
- **Planificación de Recursos Humanos**: Incluir en los planes de continuidad del negocio la planificación de recursos humanos, asegurando la disponibilidad de personal clave y la capacitación adecuada para mantener las operaciones durante situaciones de crisis.
- **Revisión y Actualización Constante**: Revisar y actualizar regularmente los planes de continuidad del negocio para asegurar que estén alineados con los cambios en el entorno empresarial y las nuevas amenazas de seguridad, y para incorporar lecciones aprendidas de simulacros y eventos reales.

Integrar la continuidad del negocio en el desarrollo e implementación de políticas de seguridad y la capacitación continua de los empleados garantiza que la empresa esté preparada para mantener la operatividad y proteger sus activos digitales incluso en situaciones adversas o de emergencia.

IMPLEMENTACIÓN

Proponemos fortalecer la seguridad de nuestra empresa a través del desarrollo e implementación de políticas de seguridad robustas y la capacitación continua de nuestros empleados. Reconocemos que una parte fundamental de la seguridad en la era digital depende del conocimiento y las prácticas de cada uno de nuestros colaboradores.
La fase de implementación la hemos divido en las siguientes fases:

EVALUACIÓN Y DIAGNÓSTICO

Identificar y comprender el estado actual de la cultura de seguridad en la organización, así como evaluar la efectividad de las políticas, procedimientos de seguridad existentes y el nivel de conocimiento y preparación del personal frente a las amenazas de seguridad cibernética.
Esto se logrará a través de una serie de evaluaciones internas, encuestas de concienciación y análisis de incidentes de seguridad previos, con el fin de desarrollar un marco de referencia claro para el diseño y la implementación de políticas de seguridad personalizadas y programas de capacitación efectivos.
El diagnóstico buscará no solo identificar áreas de riesgo y vulnerabilidad, sino también reconocer prácticas exitosas y puntos fuertes en los que se pueda apoyar la estrategia de seguridad.

Revisión de Infraestructura Actual

En la actualidad la empresa consta con:

- 4 estaciones de trabajo que son laptops con sistemas operativos Windows 11.
- Consta de un router para el acceso a los aplicativos que se manejan.
- Consta de 1 impresora
- Cámara de seguridad

Escaneo de Vulnerabilidades

Al momento de realizar el escaneo de vulnerabilidades se encontraron las siguientes:

- No se cuentan con políticas de seguridad
- La seguridad de las contraseñas es débil
- Se encontraron parches desactualizados
- Los usuarios tienen poco conocimiento sobre la importancia de la información que se maneja.

Análisis de Resultados

- **Ausencia de políticas de seguridad**:
    - La falta de políticas de seguridad indica una brecha significativa en la gestión de riesgos de seguridad de la información. Esto expone a la empresa a vulnerabilidades potenciales y aumenta el riesgo de brechas de seguridad, intrusiones o pérdida de datos confidenciales.
- **Contraseñas débiles**:
    - El uso de contraseñas débiles aumenta el riesgo de que las cuentas de usuario sean comprometidas, lo que podría llevar a la pérdida o el robo de información confidencial.
- **Parches desactualizados**:
    - Los parches desactualizados indican que el mantenimiento y la actualización de los sistemas no se están realizando de manera adecuada.
- **Usuarios con poco conocimiento sobre seguridad de la información**:

- La falta de conciencia sobre la importancia de la seguridad de la información entre los usuarios aumenta el riesgo de incidentes de seguridad, ya que pueden no reconocer las señales de posibles amenazas o no seguir prácticas de seguridad recomendadas.

PLANIFICACIÓN ESTRATÉGICA

Este objetivo guiará la creación de un marco estratégico que no solo se enfoque en las mejoras técnicas y procedimentales, sino también en el desarrollo humano y organizacional, asegurando una protección efectiva y sostenible contra riesgos de seguridad en la información.

Desarrollo del Plan de Seguridad

Implementación de Políticas de Seguridad:

Desarrollar políticas de seguridad de la información que aborden aspectos como el acceso a los sistemas, el uso de contraseñas, la protección de datos confidenciales y la respuesta a incidentes de seguridad. Estas políticas deben ser claras, concisas y comunicadas a todos los empleados de la empresa.

Mejora de Contraseñas:

- **Actualización de Parches y Software**:
  - Implementar un programa de gestión de parches para garantizar que todos los sistemas y software estén actualizados con las últimas correcciones de seguridad. Esto puede incluir la automatización de actualizaciones y la programación regular de mantenimiento para garantizar que los sistemas estén protegidos contra vulnerabilidades conocidas.
- **Capacitación y Concientización del Personal**:
  - Realizar programas de capacitación y concientización sobre seguridad de la información para todos los empleados. Esto incluirá educación sobre prácticas seguras de contraseñas, reconocimiento de correos electrónicos de phishing, manejo adecuado de datos confidenciales y procedimientos de respuesta a incidentes de seguridad.

Implementación de Medidas de Seguridad Técnica:

- Configurar firewalls, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) para proteger la red contra ataques externos e internos.
- Además, implementar soluciones de seguridad de endpoint para proteger los dispositivos de los usuarios contra malware y otras amenazas.

Auditorías y Evaluaciones de Seguridad:

- Realizar auditorías regulares de seguridad de la información para evaluar la efectividad de las medidas de seguridad implementadas y identificar posibles áreas de mejora. Estas auditorías pueden incluir pruebas de penetración, análisis de vulnerabilidades y revisiones de políticas y procedimientos.

Gestión de Incidentes de Seguridad:

- Desarrollar y documentar un plan de respuesta a incidentes de seguridad que establezca los roles y responsabilidades del personal en caso de una violación de seguridad. Esto incluirá la notificación de incidentes, la investigación, la contención, la recuperación y el análisis de lecciones aprendidas para mejorar las medidas de seguridad en el futuro.

Monitorización y Registro de Actividades:

- Implementar sistemas de monitorización de seguridad para supervisar de manera continua el tráfico de red, los registros de eventos y las actividades de usuario en busca de comportamientos sospechosos o actividades maliciosas.

Respaldo y Recuperación de Datos:

- Establecer políticas y procedimientos para realizar copias de seguridad regulares de datos críticos y desarrollar un plan de recuperación de desastres para restaurar la operación normal en caso de pérdida de datos o interrupción del sistema.

Revisión y Mejora Continua:

- Realizar revisiones periódicas del plan de seguridad para identificar áreas de mejora y adaptarse a las nuevas amenazas y tecnologías. Esto incluirá la actualización de políticas y procedimientos, así como la implementación de nuevas medidas de seguridad según sea necesario.

Implementación de Medidas Preventivas y Correctivas

- **Implementación de Políticas de Seguridad**:
  - Preventiva: Desarrollar políticas de seguridad de la información que establezcan claramente los estándares y procedimientos de seguridad que deben seguir todos los empleados.
  - Correctiva: Realizar auditorías periódicas para verificar el cumplimiento de las políticas de seguridad y tomar medidas correctivas en caso de violaciones o incumplimientos.
- **Mejora de Contraseñas**:
  - Preventiva: Implementar políticas de contraseñas que exijan contraseñas robustas y cambiantes regularmente.
  - Correctiva: Implementar un sistema de gestión de contraseñas para asegurar el cumplimiento de las políticas y cambiar las contraseñas débiles existentes.
- **Actualización de Parches y Software**:
  - Preventiva: Establecer un programa de gestión de parches para mantener actualizados todos los sistemas y software.
  - Correctiva: Realizar actualizaciones urgentes en caso de descubrimiento de vulnerabilidades críticas y programar actualizaciones regulares para mantener los sistemas al día.
- **Capacitación y Concientización del Personal**:
  - Preventiva: Proporcionar formación continua sobre seguridad de la información y concienciar a los empleados sobre las prácticas seguras.
  - Correctiva: Ofrecer formación adicional a los empleados que incumplan las políticas de seguridad y proporcionar orientación sobre cómo evitar futuras violaciones.
- **Implementación de Medidas de Seguridad Técnica**:
  - Preventiva: Configurar firewalls, IDS/IPS y soluciones de seguridad de endpoint para proteger proactivamente la red y los dispositivos.

- Correctiva: Realizar análisis de seguridad después de incidentes para identificar puntos débiles en la infraestructura y tomar medidas correctivas para fortalecer la seguridad.

- **Gestión de Incidentes de Seguridad**:
  - Preventiva: Desarrollar un plan de respuesta a incidentes de seguridad para actuar de manera rápida y eficaz en caso de una violación de seguridad.
  - Correctiva: Llevar a cabo investigaciones exhaustivas después de incidentes para identificar las causas subyacentes y tomar medidas correctivas para prevenir futuros incidentes similares.

- **Monitorización y Registro de Actividades**:
  - Preventiva: Implementar sistemas de monitorización para identificar y prevenir actividades maliciosas o sospechosas.
  - Correctiva: Revisar los registros de actividad regularmente para detectar posibles indicadores de compromiso y tomar medidas correctivas según sea necesario.

- **Respaldo y Recuperación de Datos**:
  - Preventiva: Establecer procedimientos de copia de seguridad y recuperación de datos para garantizar la disponibilidad y la integridad de la información.
  - Correctiva: Restaurar los datos desde copias de seguridad en caso de pérdida o corrupción de datos y realizar análisis de causa raíz para evitar futuras interrupciones.

- **Revisión y Mejora Continua**:
  - Preventiva: Realizar revisiones regulares del plan de seguridad y actualizarlo según sea necesario para hacer frente a las nuevas amenazas y vulnerabilidades.
  - Correctiva: Implementar medidas correctivas basadas en los hallazgos de las revisiones para mejorar continuamente la postura de seguridad de la empresa.

IMPLEMENTACIÓN

Mejorar la postura de seguridad de la empresa y proteger los activos críticos, datos sensibles y la reputación de la organización contra amenazas cibernéticas y riesgos de seguridad, asegurando la continuidad del negocio y la confianza de los clientes

Implementación de Políticas de Seguridad:

- Desarrollar políticas de seguridad de la información claras y detalladas que aborden aspectos como el acceso a los sistemas, el uso de contraseñas, la protección de datos y la respuesta a incidentes de seguridad.
- Desarrollar políticas de seguridad de la información claras y detalladas que aborden aspectos como el acceso a los sistemas, el uso de contraseñas, la protección de datos y la respuesta a incidentes de seguridad.

Mejora de Contraseñas:

- Establecer requisitos para contraseñas seguras, como longitud mínima, combinación de caracteres y cambios regulares de contraseña.
- Implementar un sistema de gestión de contraseñas para facilitar la creación, almacenamiento y gestión segura de las contraseñas.

Actualización de Parches y Software:

- Implementa un programa de gestión de parches para mantener actualizados todos los sistemas y software de la empresa.
- Automatiza el proceso de actualización cuando sea posible para garantizar que los sistemas estén protegidos contra vulnerabilidades conocidas.

Capacitación y Concientización del Personal:

- Ofrecer formación y concienciación sobre seguridad de la información a todos los empleados, incluyendo la importancia de proteger datos sensibles y reconocer posibles amenazas.

- Proporcionar ejemplos prácticos y escenarios de seguridad para ayudar a los empleados a comprender cómo aplicar las políticas de seguridad en su trabajo diario.

Implementación de Medidas de Seguridad Técnica:

- Configurar firewalls, IDS/IPS y soluciones de seguridad de endpoint para proteger la red y los dispositivos contra amenazas externas e internas.
- Realizar pruebas exhaustivas de seguridad antes de implementar nuevas medidas para garantizar su efectividad y compatibilidad con los sistemas existentes.

Auditorías y Evaluaciones de Seguridad:

- Programar auditorías regulares de seguridad para evaluar la efectividad de las medidas implementadas y identificar posibles áreas de mejora.
- Actuar sobre las recomendaciones de las auditorías y realiza un seguimiento para asegurarte de que se aborden todas las vulnerabilidades identificadas.

Gestión de Incidentes de Seguridad:

- Desarrollar un plan de respuesta a incidentes detallado que establezca los pasos a seguir en caso de una violación de seguridad.
- Realizar ejercicios de simulacro de incidentes para entrenar al personal en la ejecución efectiva del plan y mejorar la preparación para emergencias.

Monitorización y Registro de Actividades:

- Implementar sistemas de monitorización continua para supervisar la actividad de la red y los sistemas en busca de comportamientos anómalos.
- Configurar alertas automáticas para notificar al equipo de seguridad sobre posibles incidentes o actividades sospechosas.

Respaldo y Recuperación de Datos:

- Establecer un programa de copias de seguridad regular para garantizar la disponibilidad y la integridad de los datos críticos.

- Probar regularmente los procedimientos de recuperación de desastres para asegurarte de que puedas restaurar rápidamente la operación normal en caso de una interrupción del sistema.

Revisión y Mejora Continua:

- Realizar revisiones regulares del programa de seguridad para identificar áreas de mejora y adaptarte a las nuevas amenazas y tecnologías.
- Actualizar las políticas y procedimientos de seguridad según sea necesario y proporciona formación adicional al personal para garantizar la adopción continua de las mejores prácticas de seguridad.

CONCLUSIÓN

En conclusión, el fortalecimiento del desarrollo e implementación de políticas de seguridad y la capacitación continua de nuestros empleados son pilares fundamentales para garantizar la protección de los activos digitales y la resiliencia ante las crecientes amenazas cibernéticas. Al integrar políticas de seguridad robustas, que aborden tanto aspectos técnicos como comportamentales, junto con programas de capacitación que promuevan la conciencia y las habilidades en seguridad cibernética, podemos crear un entorno empresarial más seguro y preparado para enfrentar los desafíos del mundo digital.

La implementación efectiva de políticas de seguridad requiere un enfoque integral que incluya la participación de todos los niveles de la organización, desde la alta dirección hasta los empleados de base. Es crucial establecer normas claras, procedimientos efectivos y controles adecuados para mitigar riesgos y proteger la información sensible de la empresa. Al mismo tiempo, la capacitación continua de los empleados es esencial para mantenerlos actualizados sobre las últimas amenazas y mejores prácticas de seguridad, capacitándolos para identificar y responder adecuadamente a posibles ataques cibernéticos.

Al fortalecer la cultura de seguridad dentro de la empresa, no solo protegemos los activos digitales y la reputación de la organización, sino que también contribuimos a crear un entorno de trabajo más seguro y confiable para todos los empleados. En un panorama cibernético en constante evolución, el compromiso con la seguridad y la capacitación continua son elementos clave para mantenernos un paso adelante de los ciberdelincuentes y garantizar el éxito a largo plazo de nuestra empresa en la era digital.

BLIBLIOGRAFIA

Edmondson, M. D. (2017). *Global Cybersecurity: Applying International Law and Ethics.* Wiley.

Hasib, M. (2017). *Cybersecurity: A Business Solution.* Auerbach Publications.

McNeil, A. (2020). *Ciberseguridad: Protegiendo tus datos en un mundo digital.* Pearson.

Morán, J. M. (2019). *Ciberseguridad: Técnicas, tecnologías y buenas prácticas para garantizar la seguridad en la red.* Ra-Ma Editorial.

ANEXO

Enlace de evidencias de aprendizaje e implementación

https://www.notion.so/54d95f23144b4d87b3ea5290f15487e4?v=0bc148fb4f9e4f588d8b67ed08e362b0&pvs=4