COMPECER®
ORGANISMO DE CERTIFICACIÓN

SEGURIDAD DIGITAL:
¿Cómo prevenir hackeos y proteger la información de tu empresa?

¡Actúa antes de que los Hackers lo hagan!

CONTENIDO

01 **Introducción**

02 **Objetivo | Ebook**

03 Tema 1:
Introducción a la Seguridad Digital

04 Tema 2:
Tipos de Hackeos y Amenazas

05 Tema 3:
Estrategias de Prevención de Hackeos

06 Tema 4:
Medidas Prácticas para Proteger la Información

07 Tema 5:
Comunicación Externa y Controles ISO

08 Tema 5:
Capacitación continua

DESCRIPCIÓN DEL EBOOK:

En un mundo cada vez más conectado, la seguridad digital es esencial para cualquier empresa. **Este ebook proporciona estrategias prácticas para prevenir hackeos,** salvaguardar datos y mantener la integridad de la información empresarial. Desde medidas básicas hasta enfoques avanzados, descubrirás como actuar antes de que los hackers tengan la oportunidad.

OBJETIVO EBOOK

Ayudar a las empresas a fortalecer su resiliencia digital y a actuar proactivamente para evitar ser víctimas de ciberataques.

INTRODUCCIÓN A LA SEGURIDAD DIGITAL

1. Explicación de los Riesgos Actuales en el Mundo Digital
En la era digital, las empresas enfrentan una serie de riesgos que van más allá de los tradicionales. Los ciberataques pueden provenir de cualquier parte del mundo y afectar a organizaciones de todos los tamaños. Algunos de los riesgos más comunes incluyen:

Malware: Software malicioso diseñado para infiltrarse en sistemas y robar información confidencial o dañar activos digitales.
Phishing: Ataques de ingeniería social en los que los atacantes se hacen pasar por entidades legítimas para obtener datos personales o credenciales.
Ransomware: Bloqueo o cifrado de archivos a cambio de un rescate.
Violaciones de Datos: Acceso no autorizado a información sensible, como datos de clientes o empleados.

2. Estadísticas sobre Ataques Cibernéticos y sus Consecuencias Económicas
Las cifras son impactantes:
Según el informe de Verizon sobre Brechas de Datos, en 2020 se registraron más de ***20 mil millones de registros comprometidos*** debido a ataques cibernéticos.
El costo promedio de una violación de datos para una empresa es de varios millones de dólares, considerando no solo la recuperación técnica sino también la pérdida de confianza de los clientes y la reputación dañada.

3. Importancia de la Ciberseguridad como Inversión Clave
La ciberseguridad ya no es opcional; es una inversión crítica para cualquier empresa. Algunas razones clave para considerarla:

Protección de Activos Digitales: La información, los sistemas y los datos son activos valiosos. La ciberseguridad protege estos activos contra amenazas.
Cumplimiento Normativo: Muchas industrias tienen regulaciones específicas sobre seguridad de datos. Cumplir con estas normativas es esencial para evitar sanciones.
Confianza del Cliente: La seguridad es un factor importante para la confianza del cliente. Las empresas que demuestran un enfoque proactivo hacia la ciberseguridad ganan la confianza de sus clientes.

4. Noticias Grandes sobre Ataques Cibernéticos o Hackeos a Empresas
Los titulares de noticias están llenos de ejemplos de ataques cibernéticos a empresas:
SolarWinds: Un ataque masivo a través de una actualización de software afectó a numerosas organizaciones y agencias gubernamentales.
Colonial Pipeline: Un ataque de ransomware paralizó el oleoducto más grande de EE. UU., causando escasez de combustible.
JBS: El mayor procesador de carne del mundo sufrió un ataque similar, afectando la cadena de suministro de alimentos.

5. Pérdidas de Empresas no solo en lo Económico
Además de las pérdidas financieras, los ataques cibernéticos pueden tener consecuencias en la reputación, la confianza del cliente y la continuidad del negocio. Las empresas deben considerar la seguridad digital como una prioridad estratégica para proteger su futuro.

Más del 90%
de los ataques requieren de interacción humana para ser exitosos

TIPOS DE HACKEOS Y AMENAZAS

1. Ataques de Malware
Los ataques de malware son una de las amenazas más comunes y peligrosas en el mundo digital. Aquí tienes más información:

¿Qué es el Malware?: El término "malware" se deriva de ***"software malicioso"***. Se refiere a cualquier programa o código diseñado para dañar, robar o comprometer sistemas informáticos.
Infiltración: El malware puede ingresar a sistemas a través de descargas de archivos adjuntos de correo electrónico, sitios web comprometidos o dispositivos USB infectados.
Tipos de Malware:

Virus: Se propaga al adjuntarse a archivos legítimos y se activa cuando se ejecuta el archivo.
Gusanos: Se replican y se propagan automáticamente sin necesidad de intervención humana.
Troyanos: Parecen ser programas legítimos pero contienen código malicioso.
Spyware: Monitorea actividades en línea sin el conocimiento del usuario.
Ransomware: Bloquea archivos o sistemas y exige un rescate para desbloquearlos.

2. Phishing
El phishing es una técnica de ingeniería social utilizada para engañar a las personas y obtener información personal o confidencial.
Cómo Funciona:
-Los atacantes envían correos electrónicos falsificados que parecen provenir de fuentes legítimas (como bancos o empresas).
-Solicitan al destinatario que revele información confidencial, como contraseñas o números de tarjetas de crédito.
-Los enlaces en estos correos electrónicos suelen dirigir a sitios web fraudulentos.

3. Ransomware
El ransomware es una amenaza que ha afectado a muchas organizaciones.

Bloqueo de Sistemas: El ransomware cifra archivos o sistemas, impidiendo el acceso a los datos.
Demanda de Rescate: Los atacantes exigen un pago (generalmente en criptomonedas) para desbloquear los archivos o sistemas.
Impacto Económico: Las empresas pueden enfrentar pérdidas financieras significativas debido a la interrupción de operaciones y la necesidad de pagar el rescate.

4. Explotación de Vulnerabilidades
Los ciberdelincuentes buscan debilidades en el software y los sistemas para explotarlos.

Software Desactualizado: Las vulnerabilidades a menudo se encuentran en versiones antiguas de software.
Parches de Seguridad: Las empresas deben aplicar regularmente parches y actualizaciones para protegerse contra la explotación.

ESTRATEGIAS DE PREVENCIÓN DE HACKEOS

1. Autenticación Robusta
La autenticación de dos factores (2FA) es una capa adicional de seguridad que requiere más que una simple contraseña para acceder a cuentas o sistemas:

Cómo Funciona:
El usuario ingresa su contraseña como de costumbre.
Luego, se le solicita un segundo factor de autenticación, como un código enviado por SMS o una aplicación de autenticación.
Esto dificulta que los atacantes accedan incluso si conocen la contraseña.

2. Uso de Tokens o Mensajes SMS junto con Contraseñas
Tokens: Los tokens físicos o aplicaciones generan códigos únicos contraseñas.
SMS: Los mensajes de texto con códigos temporales también agregan una capa de seguridad.

3. Automatización de la Seguridad
La inteligencia artificial (IA) y el aprendizaje automático (ML) pueden mejorar la seguridad:
Detección en Tiempo Real:
Monitorea actividades sospechosas en redes y sistemas.
Detecta patrones anómalos que podrían indicar un ataque.

4. Educación y Concientización
La seguridad no es solo tecnología; también implica a las personas:
Auditoría de Seguridad:
Realiza evaluaciones regulares de riesgos y vulnerabilidades.
Identifica áreas de mejora y toma medidas correctivas.

5. Plan de Continuidad del Negocio
Desarrollo de un Plan:
Define cómo mantener operaciones incluso después de un ataque.
Incluye respaldo de datos, sistemas redundantes y comunicación con partes interesadas.

6. Implementación de Herramientas en la Nube y Uso de Aplicaciones Seguras
Google Workspace:
Utiliza herramientas en la nube como Google Drive y Gmail.
Configura permisos adecuados y realiza copias de seguridad.

MEDIDAS PRÁCTICAS PARA PROTEGER LA INFORMACIÓN

1. Copia de Seguridad de Datos

Realización Regular de Copias de Seguridad:

Programa copias de seguridad automáticas y frecuentes.
Almacena copias en ubicaciones seguras, como servidores externos o la nube.
Verifica periódicamente que las copias sean accesibles y estén actualizadas.

2. Contraseñas Seguras y Autenticación Multifactor

Contraseñas Complejas y Únicas:

Evita contraseñas obvias como “123456” o “contraseña”.
Combina letras mayúsculas, minúsculas, números y caracteres especiales.
Utiliza administradores de contraseñas para gestionarlas de manera segura.
Implementación de 2FA (Autenticación de Dos Factores):
Activa 2FA en todas las plataformas y servicios.
Esto requiere un segundo factor (como un código enviado al teléfono) además de la contraseña.

3. Desconfianza de Correos Electrónicos de Desconocidos

Evitar Abrir Correos Sospechosos:

No hagas clic en enlaces ni descargues archivos adjuntos de remitentes desconocidos.
Verifica la dirección de correo electrónico y busca señales de phishing, como errores ortográficos o solicitudes inusuales.

4. Actualización de Antivirus y Antimalware

Mantener los Sistemas Protegidos:

Instala y actualiza regularmente software antivirus y antimalware.
Escanea sistemas en busca de amenazas y elimina cualquier malware detectado.

5. Medidas Técnicas y Operativas

Firewalls y Antivirus:

Configura firewalls para filtrar el tráfico no deseado.
Asegúrate de que todas las computadoras tengan software de seguridad actualizado.

Copias de Seguridad Regulares:

Realiza copias de seguridad de datos críticos y almacénalas fuera del sitio.
Prueba la restauración de datos para verificar su integridad.

Actualizaciones de Software:

Mantén sistemas y aplicaciones actualizados para evitar vulnerabilidades conocidas.

6. Capacitación del Personal

Sesiones de Capacitación:

Ofrece formación sobre phishing, contraseñas seguras y uso seguro de dispositivos.
Educa a los empleados sobre las amenazas y cómo protegerse.

7. Simulacros de Ataque

Preparación ante Incidentes:

Realiza ejercicios simulados para que los empleados practiquen respuestas ante ataques.
Evalúa la efectividad de los planes de seguridad y ajusta según los resultados.

COMUNICACIÓN EXTERNA Y CONTROLES ISO

1. Comunicación Externa y Relaciones Públicas
La comunicación externa es crucial para mantener la confianza de los clientes y socios:
Transmitir Confianza:
Comunica de manera proactiva las medidas de seguridad implementadas.
Destaca el compromiso de la empresa con la protección de datos y la resiliencia.

2. Comunicados de Prensa
Transparencia en Incidentes:
Si ocurre un incidente de seguridad, emite un comunicado de prensa.
Describe las acciones tomadas para mitigar el impacto y proteger a los afectados.

3. Redes Sociales y Sitio Web
Publicaciones Regulares:
Utiliza redes sociales y el sitio web para compartir actualizaciones sobre medidas de seguridad.
Destaca logros en resiliencia, como la implementación de controles ISO.

4. Referencias a ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad.
Fortalecimiento de la Resiliencia:
La certificación **ISO/IEC 27001:2022** es un estándar reconocido internacionalmente para la gestión de seguridad de la información, su objetivo es establecer un sistema de gestión de seguridad de la información (SGSI) que garantice la confidencialidad, integridad y disponibilidad de los datos. Esta norma proporciona pautas para gestionar riesgos y controlar la seguridad de la información en cualquier tipo de organización, ya sea grande o pequeña, pública o privada.
Menciona cómo los controles de la ISO 27001 contribuyen a la resiliencia de la empresa.

5. Beneficios de la Certificación ISO/IEC 27001:2022
-Mejora de la seguridad de la información.
-Reducción de riesgos financieros.
-Cumplimiento legal y regulatorio.
-Acceso a nuevos mercados.
-Protección de la reputación.

6. Historias de Éxito
Ejemplos Reales:
Comparte casos de empresas que mejoraron su resiliencia mediante la certificación ISO.
Destaca cómo superaron desafíos y se recuperaron de incidentes.

CAPACITACIÓN CONTINUA

En el mundo digital actual, **la seguridad de la información es crucial** para proteger tu empresa contra hackeos y amenazas cibernéticas. Te invitamos a participar en nuestros webinars y eventos de ciberseguridad, diseñados para ayudarte a adentrarte en el mundo digital de manera segura y efectiva.

Próximo Webinar Internacional: Seguridad Digital
Fecha: 22 de agosto de 2024
Organizado por: Compecer

Descripción: Únete a nosotros en este webinar donde expertos en ciberseguridad compartirán estrategias y mejores prácticas para proteger la información de tu empresa. Aprenderás cómo prevenir hackeos y mitigar amenazas cibernéticas.

Beneficios de Participar:

Conocimiento Actualizado: Mantente al día con las últimas tendencias y técnicas en ciberseguridad. Expertos en el Tema: Aprende de profesionales con amplia experiencia en el campo.

Red de Contactos: Conéctate con otros profesionales y empresas interesadas en la seguridad digital.

Implementación Práctica: Obtén consejos prácticos que puedes aplicar inmediatamente en tu empresa.

Asegúrate de reservar tu lugar para el webinar del 22 de agosto de 2024. **¡No te lo pierdas!**

www.compecer.com