



CONTRALORÍA GENERAL
DEL QUINDÍO

Nociones Seguridad informatica

Facilitador: Donald Rodrigo
Altamirano Vasco

Junio /2024

AGENDA

1. Introducción a la Seguridad Informática
2. Tipos de Amenazas Informáticas
3. Ejemplos de Ataques Informáticos a Empresas Públicas o del Estado
4. Medidas de Seguridad Informática
5. Protocolos de Respuesta a Incidentes
6. Buenas Prácticas en Seguridad Informática por parte del personal
7. Preguntas y Respuestas



01

Introducción a la Seguridad Informática



1.Introducción a la Seguridad Informática

- **Definición:** La seguridad informática es la práctica de proteger los sistemas, redes y datos de ataques, daños y acceso no autorizado. Involucra la implementación de medidas preventivas y reactivas para salvaguardar la integridad, disponibilidad y confidencialidad de la información.
- **Objetivos:** Garantizar la protección de los datos sensibles de la Contraloría General del Quindío, mantener la continuidad operativa, y asegurar la confianza de los ciudadanos en los procesos de auditoría y control.

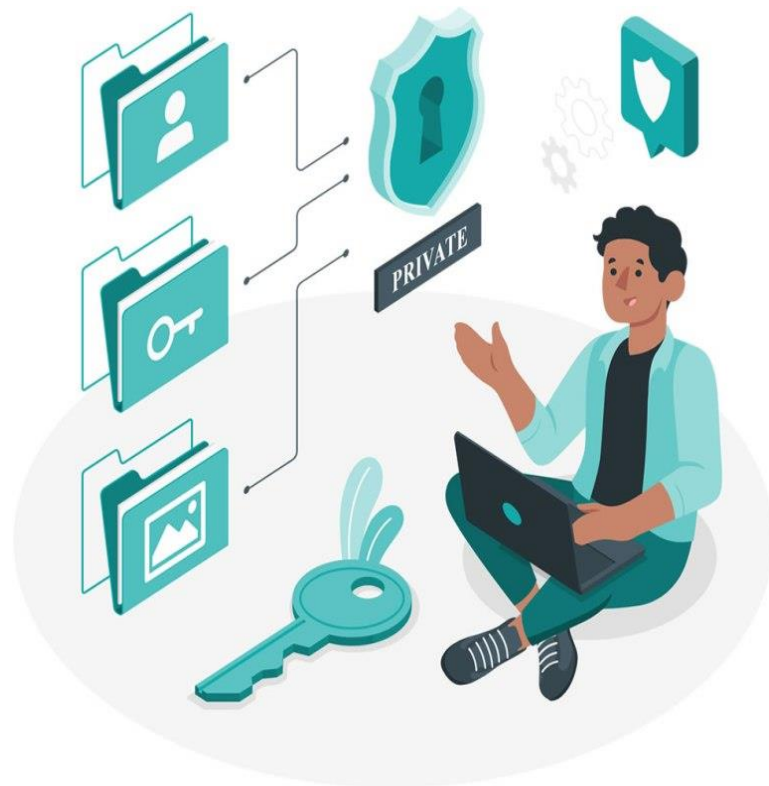


1.Introducción a la Seguridad Informática

● Importancia en el Entorno Actual

La seguridad informática es crucial en el entorno actual debido al aumento constante de ataques cibernéticos y la digitalización de procesos y datos sensibles. Las organizaciones, especialmente las públicas, manejan información crítica y personal que debe ser protegida para mantener la confianza del público y la continuidad operativa.

- ✓ Protección de Datos Personales
- ✓ Prevención de Pérdidas Financieras
- ✓ Cumplimiento Normativo
- ✓ Reputación y Confianza



1.Introducción a la Seguridad Informática - Breve Historia de la Seguridad Informática

Comienzan a surgir las primeras preocupaciones sobre la seguridad de las computadoras, con investigaciones en seguridad de sistemas operativos.

1970

2000

Expansión masiva de internet y la globalización del comercio electrónico, lo que lleva a un incremento significativo en la cantidad y sofisticación de ataques cibernéticos.

Aumenta la conectividad de las computadoras y se empiezan a ver los primeros virus informáticos, como el famoso "Elk Cloner".

1980

2010

Aparición de ataques de alto perfil como el ransomware WannaCry, que afectó a organizaciones de todo el mundo.

Crecimiento de internet y aparición de amenazas más sofisticadas, como los primeros ataques de phishing.

1990

**2020
y mas**

Las amenazas cibernéticas se vuelven más sofisticadas y los ataques a infraestructuras críticas, como los sistemas de salud y gobierno, se vuelven más comunes.

1.Introducción a la Seguridad Informática

Ejemplos de Vulnerabilidades en Colombia

2019



Vulnerabilidad: Exposición de datos personales de millones de ciudadanos debido a una configuración incorrecta de la base de datos.

Impacto: Riesgo de robo de identidad y uso indebido de datos personales.

Lección Aprendida: Importancia de la configuración segura y el monitoreo constante de las bases de datos

 El Espectador

Registraduría confirma que fue un ataque cibernético la caída de su página

También se habría presentado una acción en contra de un aplicativo del Consejo Nacional Electoral.



1.Introducción a la Seguridad Informática

Ejemplos de Vulnerabilidades en Colombia



ALCALDÍA MAYOR
DE BOGOTÁ D.C.

2020

Vulnerabilidad : Acceso no autorizado a registros médicos a través de fallos en el sistema de seguridad.

Impacto: Exposición de información médica confidencial

Lección Aprendida: Necesidad de fortalecer la seguridad en sistemas que manejan datos sensibles y asegurar la protección de la privacidad de los usuarios.

2021

Vulnerabilidad : Ataque de ransomware que afectó los servicios en línea y el acceso a datos importante

Impacto: Interrupción de servicios públicos y posibles pérdidas de datos críticos

Lección Aprendida: Importancia de las copias de seguridad regulares y la implementación de soluciones efectivas de recuperación ante desastres.

1.Introducción a la Seguridad Informática

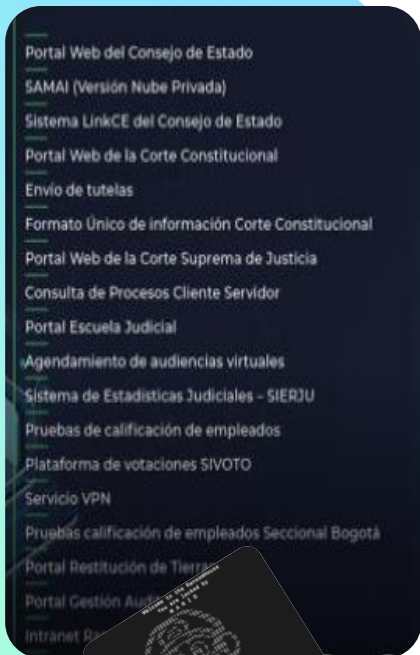
Ejemplos de Vulnerabilidades en Colombia

2023

Vulnerabilidad : IFX Networks Colombia S.A.S. sufrió un ataque de ransomware que comprometió una parte importante de su infraestructura tecnológica.

Impacto: el ataque afectó los servicios de comunicación y red que la empresa ofrece a sus clientes, incluyendo empresas privadas y entidades públicas. La recuperación de los datos y la restauración completa de los servicios tomaron semanas, lo que generó una significativa interrupción operativa y pérdidas económicas.

Lección Aprendida: La necesidad de tener una robusta estrategia de ciberseguridad que incluya copias de seguridad regulares, segmentación de la red para limitar la propagación de malware, y planes de respuesta a incidentes bien definidos y probados. Además, subraya la importancia de educar continuamente al personal en prácticas de seguridad para reducir el riesgo de ser víctimas de phishing y otros vectores de ataque



02

TIPOS DE AMENAZAS INFORMATICAS



2.1 AMENAZAS INFORMATICAS - MALWARE

Viene de la combinación de las palabras "malicioso" y "software". Se refiere a programas de computadora diseñados para dañar, robar información o hacer funcionar mal tu dispositivo sin tu permiso.

Ejemplos de vulnerabilidades que pueden llevar a la amenaza de malware:

- Descargas desde fuentes no confiables
- Actualizaciones no realizadas.
- Hacer clic en enlaces maliciosos
- Uso de dispositivos USB infectados

<https://www.youtube.com/watch?v=HuasitV4lcw&t=25s>
https://www.youtube.com/watch?v=HG_cvjRT5Ms



2.2 AMENAZAS INFORMATICAS - Phishing

Es una forma de engaño en línea donde los estafadores intentan obtener información confidencial, como contraseñas o detalles de tarjetas de crédito, haciéndose pasar por entidades de confianza. Usualmente lo hacen a través de correos electrónicos, mensajes de texto o llamadas telefónicas que parecen legítimos.

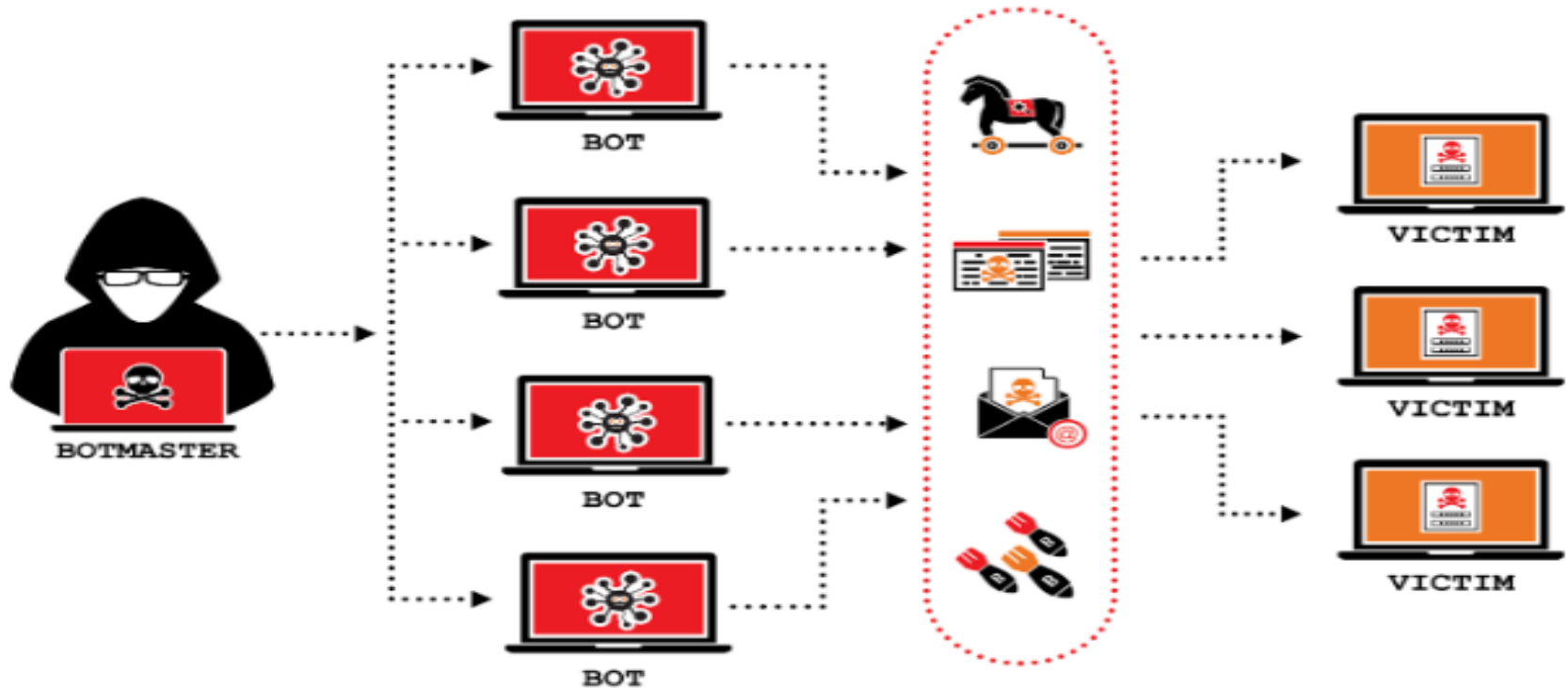
Ejemplos de vulnerabilidades que pueden llevar a la amenaza de Phishing:

- Falta de conocimiento sobre el phishing
- Falta de atención a los detalles
- Confianza excesiva en los remitentes
- Falta de medidas de seguridad en el correo electrónico

<https://www.youtube.com/watch?v=UuuAIP7ay6>



2.3 Ataques de denegación de servicio (DDoS)



<https://www.youtube.com/watch?v=7xGdz5Li9Sw>

2.4 Ingeniería social

son como trucos o engaños que utilizan los delincuentes cibernéticos para obtener información confidencial o acceso a sistemas informáticos. En lugar de atacar directamente a un sistema, intentan engañar a las personas para que revelen información sensible o realicen acciones que comprometan la seguridad.

Ejemplos de vulnerabilidades que pueden llevar a la amenaza Ingeniería social

- Phishing : Email idénticos a las entidades gubernamentales o financieras solicitando cambios de claves o actualizaciones
- Suplantación de identidad por redes sociales (whatsapp, Instagram, Facebook)
- Ofertas Falsas
- Sextorsion
- Solicitud de Ayudas urgentes
- Sms

Pueden buscar los mas vulnerables (familia)

<https://www.youtube.com/watch?v=AQG1sHLiqSA>



3. Ejemplos de Ataques Informáticos a Empresas Públicas o del Estado

EMPRESAS QUE HAN SIDO HACKEADAS

04

Medidas de Seguridad Informatica



4. Medidas de Seguridad

Actualizaciones de software y gestión de parches

Son medidas fundamentales en seguridad informática para proteger sistemas y datos contra vulnerabilidades conocidas tanto para la empresa como a nivel personal. Consisten en aplicar correcciones y mejoras proporcionadas por los fabricantes de software para cerrar brechas de seguridad y mejorar el rendimiento de los programas.

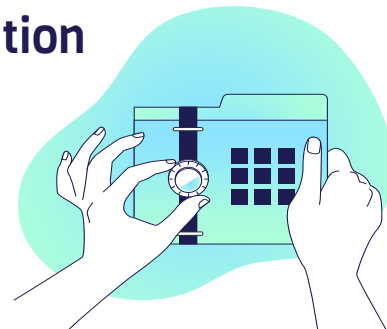
- Identificación de vulnerabilidades
- Evaluación de impacto
- Desarrollo de políticas
- Implementación de parches
- Pruebas y validación
- Seguimiento y auditoría



Problem



Solution



4. Medidas de Seguridad- El uso de antivirus y antimalware

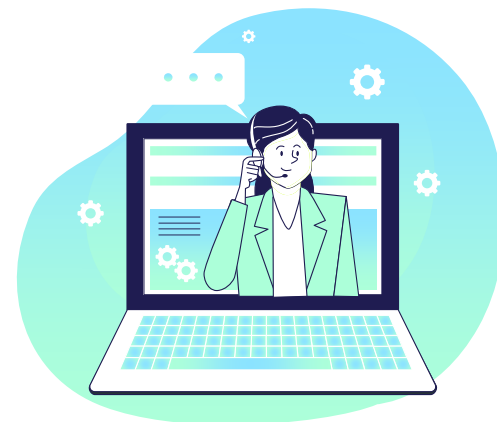
Es fundamental en seguridad informática tanto a nivel empresarial como personal, ya que ayudan a proteger contra amenazas como virus, malware, ransomware y otras formas de software malicioso.

Empresas

- Soluciones de seguridad robustas que no afecten el rendimiento del equipo.
- Deben verificar en tiempo real la validación de ingreso de medios externos (USB, conexión por bluetooth, Wifi – Free)
- Realizar ingeniería social preventiva a los funcionarios para ver su nivel de conciencia con la seguridad informática.

Personal

- Disp. Móviles – portátiles personales con acceso empresarial.



4. Medidas de Seguridad

Implementación de firewalls y sistemas de detección de intrusos

Un firewall es un dispositivo de seguridad de red que monitorea y controla el tráfico de red entrante y saliente basado en reglas de seguridad predefinidas.

Un IDS es una herramienta de seguridad que monitorea la red y los sistemas en busca de actividades sospechosas o maliciosas y envía alertas cuando detecta posibles intrusiones.

Empresas: puede usar un NGFW para proteger sus servidores y datos confidenciales, bloqueando el acceso no autorizado y filtrando contenido malicioso.

Personal: Configurar el firewall de su router para bloquear ciertos puertos y servicios que no utiliza



4. Medidas de Seguridad

Importancia de las copias de seguridad (backups):

Son duplicados de datos importantes que se almacenan en una ubicación diferente a la original. Su propósito es proteger la información contra pérdidas accidentales, fallos del sistema, ataques cibernéticos, o desastres naturales.

Empresas

- Copias en la Nube
- Copia de Seguridad local y externa
- Copias de Seguridad Incrementales y Diferenciales

Personas

- Copias seguridad Nube
- Discos Duros Externos
- Software copias de seguridad



4. Medidas de Seguridad

Capacitación y concientización de los empleados



Es un proceso continuo y fundamental que busca educar a todos los miembros de una organización sobre las mejores prácticas para proteger la información y los sistemas contra amenazas cibernéticas.

Empresas

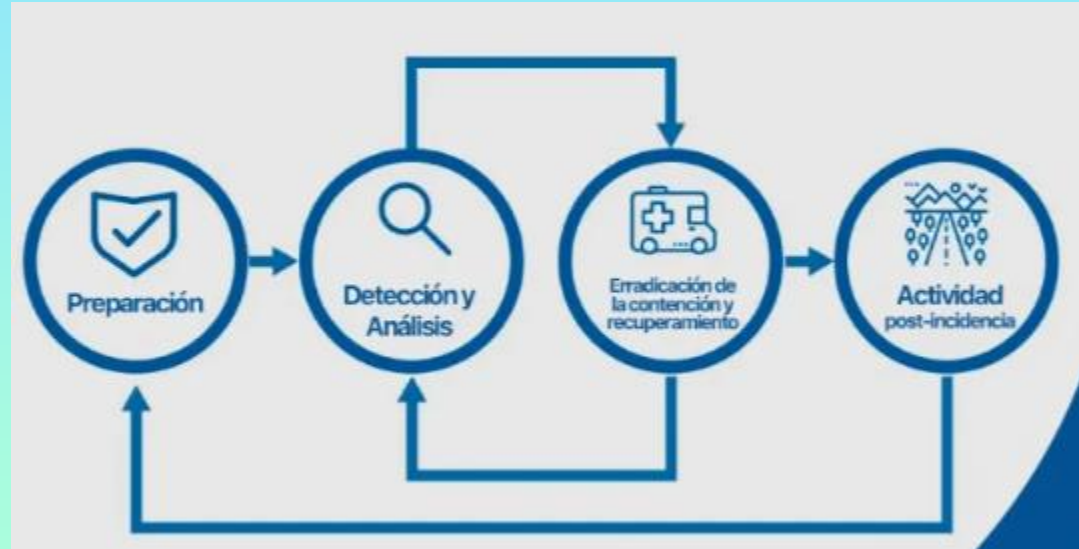
- Programas de Capacitación Regular
- Campañas de Concientización
- Simulaciones de Phishing
- Políticas de Seguridad Claras



Personal

- Autoeducación en Seguridad Informática
- Prácticas Seguras en el Uso de Internet

05 Protocolo Respuesta incidentes



5. Medidas de Seguridad

Protocolos de Respuesta a Incidentes



Son conjuntos de procedimientos y acciones predeterminadas que una organización o individuo debe seguir cuando se detecta un incidente de seguridad.

- Equipo de Respuesta a Incidentes (IRT)
- Planes de Respuesta Detallados
- Simulaciones y Ejercicios de Respuesta
- Comunicación y Notificación

06 Buenas Practicas Seguridad Informática



6. Buenas Practicas Seguridad Informatica

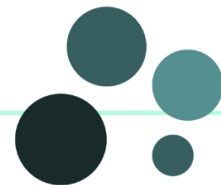
1. No ingresar memorias USB externas no autorizadas.
2. No acceder a portales web no autorizados o sospechosos.
3. Usar contraseñas seguras y únicas para cada cuenta y cambiarlas regularmente.
4. No compartir contraseñas con nadie y evitar escribirlas en lugares visibles.
5. Mantener el software y los sistemas operativos actualizados.
6. Utilizar autenticación de dos factores (2FA) para mayor seguridad.
7. No descargar ni abrir archivos adjuntos de correos electrónicos sospechosos o desconocidos
8. No hacer clic en enlaces de correos electrónicos o mensajes de fuentes no confiables
9. Usar software antivirus y antimalware actualizado y realizar escaneos periódicos.
10. No instalar software no autorizado en los dispositivos de la empresa.
11. Realizar copias de seguridad (backup) periódicas de la información crítica.
12. Bloquear la pantalla del computador al dejar el puesto de trabajo, incluso por periodos cortos.
13. Utilizar redes seguras y evitar conectarse a redes Wi-Fi públicas o no seguras.
14. Ser cauteloso con la información que se comparte en redes sociales y plataformas públicas.
15. Participar en capacitaciones y actualizaciones sobre seguridad informática.



6. Buenas Practicas Seguridad Informatica

16. No conectar dispositivos personales (teléfonos, tablets, etc.) a la red de la empresa sin autorización.
17. Evitar el uso de correos personales para asuntos laborales.
18. Ser consciente de las políticas y procedimientos de seguridad de la empresa y cumplirlos rigurosamente.
19. Reportar cualquier actividad sospechosa o incidentes de seguridad inmediatamente al departamento de TI.
20. No reutilizar contraseñas para diferentes cuentas o servicios.
21. Utilizar conexiones VPN (Red Privada Virtual) para acceder a la red de la empresa desde ubicaciones remotas.
22. Evitar el uso de servicios de almacenamiento en la nube no autorizados para guardar o compartir información de la empresa.
23. No utilizar dispositivos de la empresa para actividades personales o recreativas.
24. Revisar y seguir las directrices de seguridad específicas proporcionadas por el departamento de TI.
25. Eliminar adecuadamente la información sensible de los dispositivos antes de descartarlos o transferirlos.





CONTRALORÍA GENERAL
DEL QUINDÍO

Ping: 04907445

<https://kahoot.it/challenge/04907445>



Muchas Gracias.