¿CÓMO ENFRENTAR LOS RIESGOS DE LA **CIBERSEGURIDAD?**

Fernando Martín del Campo
Product Manager
fmc@ids-ac.com

Agenda

Bienvenida Lic. Juan Pablo Montoya
Presidente REDCAMIF

Casos reales

Evolución del Malware

¿Cómo protegerse del ransomware?

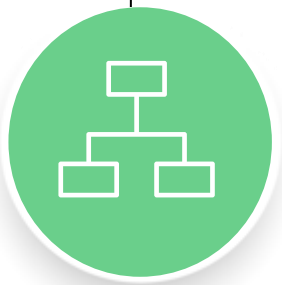
¿Cómo recuperarse de un posible ransomware?

Conclusión

Preguntas y Respuestas de la audiencia

Agradecimiento y cierre del webinar

¿Por qué Grupo I3 ?®



FACILITADOR TECNÓLOGICO

Somos un facilitador tecnológico enfocado en proveer soluciones para diversos rubros con un **alto grado de innovación, seguridad y especialización.**

POTENCIALIZADOR

Ayudamos a **potenciar el crecimiento de su Institución** por medio de la transformación digital.

EXPERIENCIA

Aportamos nuestra **experiencia de 40 años** y presencia continua en el mercado regional.

IDS - GRUPO I3 SU MEJOR ALIADO DE NEGOCIOS

Un imperativo Estratégico para la Alta Dirección

La Alta Dirección debe estar plenamente consciente que los ciberataques son una seria amenaza para la organización.

Un ciberataque incluye virus, ransomware, spyware, gusanos y otros tipos de código malicioso.

- El cambio en las preferencias de los clientes obliga a tener un modelo de multicanalidad.

- La ciberseguridad debe ser una prioridad del negocio e incorporarla a la estrategia.

- Se estima que en el **2025** las pérdidas por el cibercrimen ascenderán a **$10,500 millones** en EE.UU

→

CASOS REALES

2017

Ataque a la empresa de Logística Maersk **impactó en pocos minutos las aplicaciones de 50,000** computadoras.

2021

Facebook **comprometió la información de más de 530 millones de usuarios.**

2022

Gobierno de Costa Rica fue atacado a tal punto que se **declaró en estado de emergencia.**

2023

Ataque a Real Estate Wealth Network, **comprometió 1.16 TB de datos de más de 1,500 millones de registros.**

CASOS REALES EN INSTITUCIONES FINANCIERAS

2019

El **Banco Nación en Argentina** fue atacado, se cambió el tipo de cambio del dólar y **se realizaron transacciones de compra y venta.**

2021

El 11 de octubre el **Banco Pichincha del Ecuador** se vio obligado a cerrar gran parte de su **red de cajeros automáticos y su banca en línea.**

2023

El **Banco de México** publicó que un ataque en julio a una **Sociedad Cooperativa de Ahorro y Préstamo** les **afectó en US$1.2 millones.**

2024

El **Banco Santander** sufrió un **robo de información confidencial** que los delincuentes pusieron a la venta.

Evolución del Malware

Malware distribution/ spreading (aaS)

OPSEC (aaS)

Scamming (aaS)

Spamming (aaS)

Access (as-a-service) o aaS

Phishing (aaS)

Crypting (aaS)

Vishing (aaS)

Scanning (aaS)

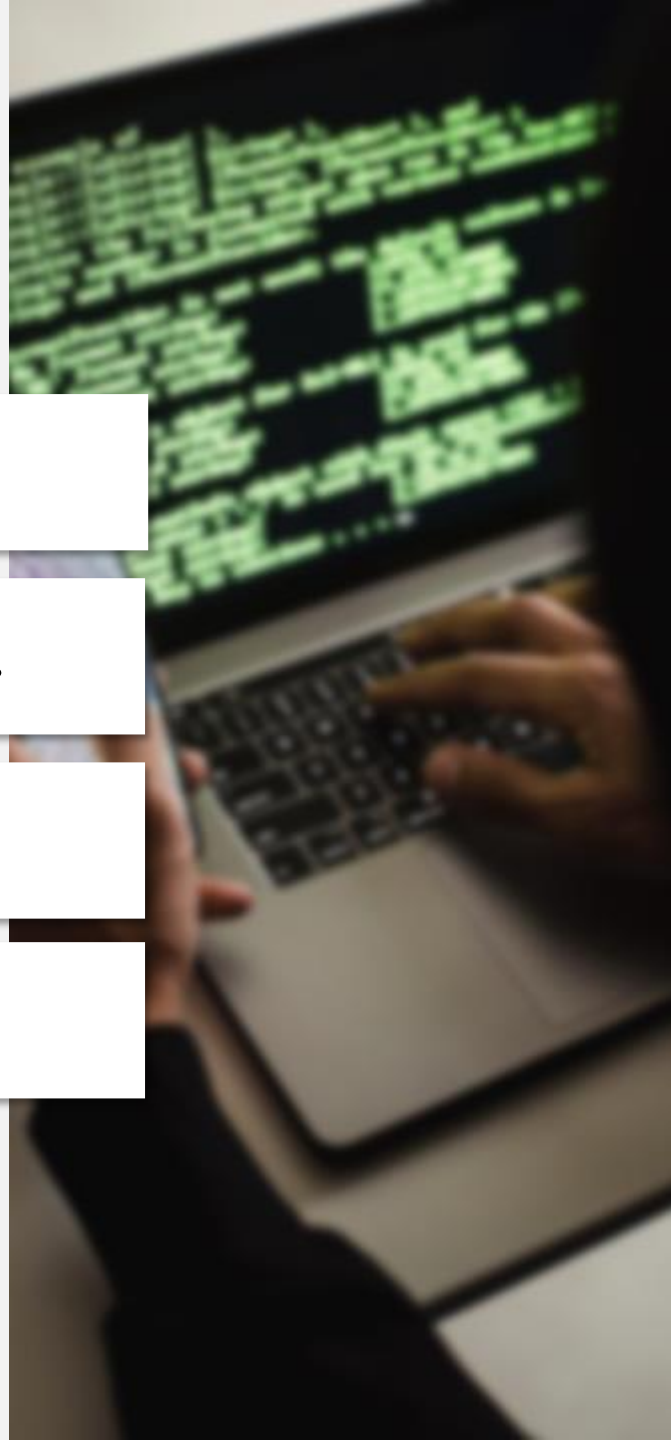
Pasos rápidos para PROTEGERSE de la amenaza del ransomware

01 Usar un software antivirus en todo momento.

02 Mantener las computadoras actualizadas y con parches.

03 Bloquear el acceso a sitios de ransomware.

04 Permitir solo aplicaciones autorizadas.



Pasos rápidos para PROTEGERSE de la amenaza del ransomware

05 Restringir el uso de dispositivos de propiedad personal.

06 Usar cuentas de usuario estándar.

07 Evitar el uso de aplicaciones personales.

08 Cuidado con las fuentes y contactos desconocidos.

RECOMENDACIONES

Soluciones y procesos que se deberían implementar

- Copia robusta de seguridad de datos (DB).
- Gestionar el navegador web y filtrado de sitios permitidos (BM).
- Prevención y concientización sobre phishing (PP).
- Monitoreo de perímetro de la red (NM).
- Gestión de los Activos tecnológicos (AM).
- Gestión de parches y actualizaciones (PM).
- Gestión de usuarios y accesos (UM).
- Integridad de las aplicaciones y listas de permisos (AI).
- Respuesta a incidentes (IR).
- Gestión de Riesgos (RM).

Descarga: https://www.cisa.gov/sites/default/files/2024-05/StopRansomware-Guide-508C-v3_1_ES.pdf

RECOMENDACIONES

- Plan de respuesta a incidentes.
- Gestión de la comunicación ante un incidente.
- Recuperación ante desastres.
- Ejercicios y simulacros dos veces al año.
- Respuesta a incidentes físicos (incendio, motines).
- Gestión del ambiente redundante.

Descarga: https://www.cisa.gov/sites/default/files/2024-05/StopRansomware-Guide-508C-v3_1_ES.pdf

Procedimientos documentados

Pasos para RECUPERARSE de un posible ataque ransomware

- Elaborar un plan de recuperación de incidentes.
- Tener copias de seguridad y restauración.
- Publicar un listado actualizado de contactos.

https://www.cisa.gov/sites/default/files/publications/data_backup_options.pdf
https://www.dpbestflow.org/backup/backup-overview#321

Conclusión

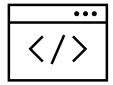
Si bien no existe una defensa segura contra todas las amenazas, también es cierto que pueden evitarse mediante:

Estrategia

- Establecer una estrategia de protección cibernética.
- La ciberseguridad debe reducir el riesgo y optimizar las capacidades de las Instituciones.

Talento y Cultura

- La implementación de ciberseguridad por parte los líderes de negocios.
- Promover la cultura de expertos en ciberseguridad.
- Capacitaciones necesarias o incorporar a proveedores de servicios.



Tecnología

- El diseño de la base digital debe incluir seguridad.
- Es importante que las Instituciones aseguren los datos del cliente.

Ecosistemas

- Comprender y gestionar los riesgos externos.
- Practicar constantemente la evaluación de ciber riesgos.
- Realizar simulacros
- Monitorear para detectar y contener amenazas.

¡Gracias por su atención!

Estamos aquí para ayudarte.

Guatemala
PBX: (+502) 2412-4212

El Salvador
PBX: (+503) 2248-5500

info@ids-ac.com
www.i3-ac.com