TECNOLOGIAS DE LA INFORMACION Y CUBERSEGURIDAD

Inacap

Tipos de Vulnerabilidad según activos TI

Seguridad de la Información

Inacap

Clasificación vulnerabilidades

Las vulnerabilidades en los activos de TI se pueden clasificar en función de varios criterios, que incluyen la naturaleza del activo y la naturaleza de la vulnerabilidad.

Inacap

Software

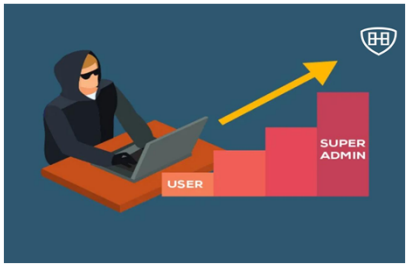
Vulnerabilidades de Aplicación
Inyección de SQL: Ataques que inyectan código SQL en consultas de la base de datos.
Cross-Site Scripting (XSS): Inyección de scripts en páginas web que se ejecutan en el navegador del usuario.
Cross-Site Request Forgery (CSRF): Manipulación de solicitudes para ejecutar acciones no deseadas en una aplicación web en nombre del usuario autenticado.

Acceder a datos confidenciales
Modificar o eliminar información
Ejecutar comandos peligrosos en el servidor
Tomar control total de la base de datos.

nacap

Software

Vulnerabilidades de Sistema Operativo
Desbordamiento de buffer: Explotación de límites de memoria para ejecutar código malicioso.
Escalada de privilegios: Aprovechamiento de fallos en el sistema para obtener privilegios más altos.



nacap

Hardware

Hardware
Manipulación directa: Acceso no autorizado a los componentes físicos.
Ataques de canal lateral: Uso de emisiones físicas (como energía o radiación) para obtener datos sensibles.
Firmware _: Exploits de firmware: Fallos en el software embebido que permiten modificar el funcionamiento del hardware.

Networking

Vulnerabilidades de protocolo
Ataques Man-in-the-Middle (MitM): Intercepción y posible alteración de la comunicación entre dos partes.
Inyección de paquetes: Introducción de datos falsificados en la red.

Vulnerabilidades de Configuración
Configuración insegura: Configuraciones por defecto o malas prácticas que dejan abiertas puertas a ataques.

Networking

Vulnerabilidades WI FI
Crackeo de claves Wi-Fi: Explotación de vulnerabilidades en protocolos de seguridad inalámbricos.

nacap

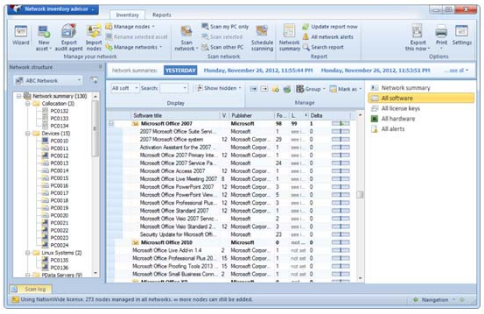
Bases de Datos

Exposición de datos: Configuraciones o errores que permiten el acceso no autorizado a los datos.
Pérdida de integridad de Datos: Ataques que alteran los datos de manera no autorizada.
Fuga de datos: Extracción no autorizada de datos sensibles o privados.

nacap

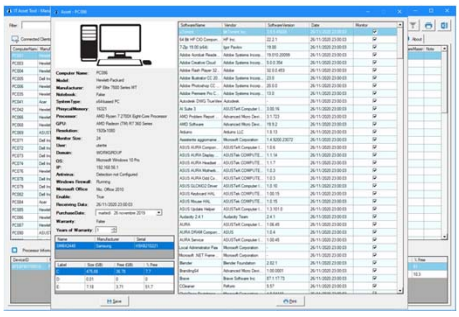
Identificación activos /Software

Activos
Inventario de aplicaciones, sistemas operativos, y herramientas.
Evaluación de la criticidad basada en la función y los datos que manejan.



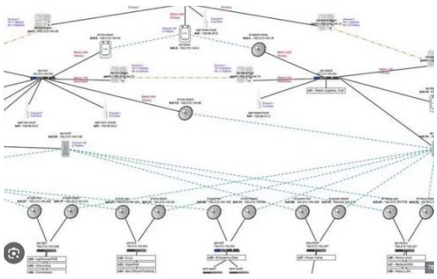
Identificación activos /hardware

Los Fierros
Registro de servidores, equipos de red, dispositivos de almacenamiento.
Evaluación del valor en función de la operación y datos almacenados.



Identificación activos /redes

Networking
Mapeo de dispositivos de red, segmentos de red, y configuraciones.
Identificación de puntos críticos y nodos vulnerables.



nacap

Identificación activos /BD

Inventario de bases de datos, sistemas de gestión de bases de datos (DBMS).
Clasificación según la sensibilidad y el volumen de datos.

nacap

Identificación activos /humanos

Las personas
Listado de usuarios, roles y permisos.
Evaluación de la criticidad basada en acceso y roles desempeñados

Clasificación

La clasificación de activos es un paso crucial en la gestión de la seguridad de la información, que implica categorizar los recursos de una organización según su importancia y el impacto potencial de su pérdida o compromiso.

Este proceso ayuda a determinar las prioridades de protección y asignar los recursos adecuados para salvaguardar los activos más críticos.

Clasificación típica

Tipo	Descripción
Críticos	que son esenciales para la operación continua de la organización.
Activos sensibles	que manejan información confidencial o personal.
Activos No críticos	cuya pérdida no afectaría severamente las operaciones.

Una correcta clasificación permite a las organizaciones implementar estrategias de seguridad más efectivas y optimizar sus esfuerzos en la gestión de riesgos.

Identificación de riesgos de relación según el tipo de industria y activos TI

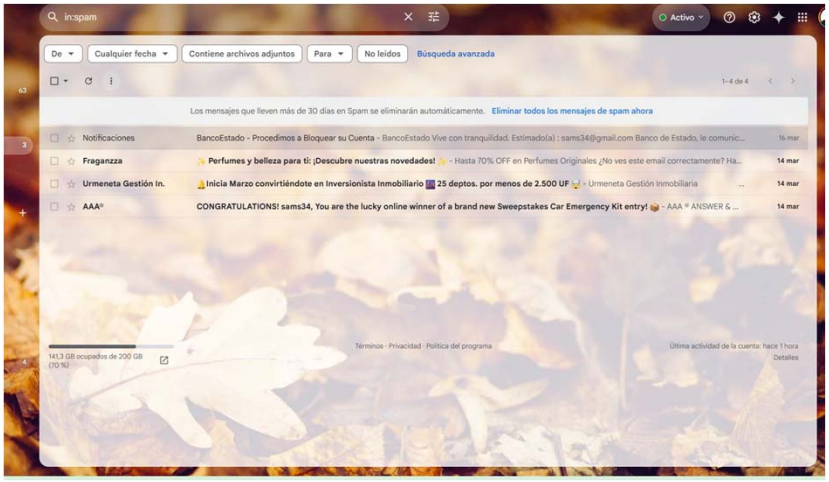
La **identificación de riesgos** de relación varía considerablemente según el tipo de industria y los activos de información involucrados

Industria financiera

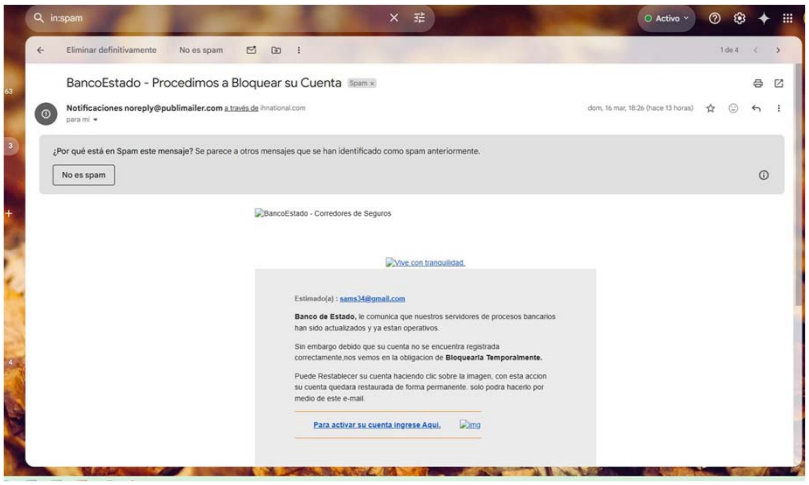
Activos
Datos financieros: Transacciones, registros de clientes, datos de tarjetas de crédito.
Sistemas de transacciones: Plataformas de trading, sistemas de pago.

Fraude y robo de identidad: Acceso no autorizado a información financiera que puede ser usado para fraude.
Ataques de phishing: Engaños para obtener credenciales de acceso a cuentas financieras.
Robo de datos: Ataques dirigidos a extraer datos financieros sensibles.

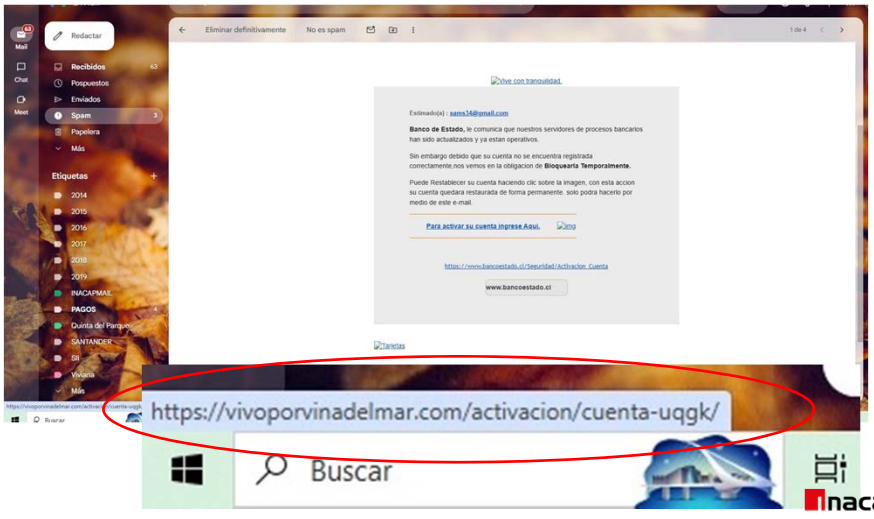
Caso Phishing



Caso Phishing



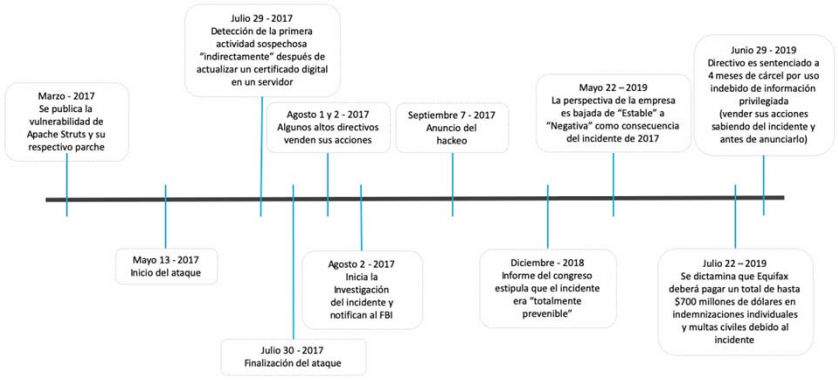
Caso Phishing



Caso Equifax - 207

En 2017, Equifax sufrió una violación de datos que expuso la información personal de millones de personas. Los piratas informáticos accedieron a los sistemas de la empresa durante varios meses antes de que la empresa se diera cuenta

Caso Equifax - 207



Sector Salud

- Registros de Salud Electrónicos (EHR): Información médica de pacientes.
- Sistemas de Diagnóstico y Tratamiento: Equipos médicos conectados.

Sector Salud / Riesgos

- Exposición de Datos de Pacientes: Fugas de información que pueden dañar la privacidad de los pacientes.
- Interrupción de Servicios Médicos: Ataques a sistemas críticos que afectan la atención médica.

Sector Tecnología y Telecomunicaciones

Activos de Información

- Datos de usuario: Información personal y de comportamiento de los usuarios.
- Infraestructura de red: Servidores, routers, y otros equipos de red.

Sector Tecnología y Telecomunicaciones

Riesgos de relación

- Interceptación de datos: Escuchas no autorizadas o captura de datos transmitidos.
- Compromiso de infraestructura: Ataques a la infraestructura de red que afectan la conectividad y el servicio.

Caso Yahoo!

Ataque a Yahoo (2013-2014): Robaron información de más de 3 mil millones de cuentas de usuario debido a la explotación de vulnerabilidades en su infraestructura.

El portal de internet Yahoo informó este miércoles que 1.000 millones de cuentas de usuarios fueron afectadas por un caso de intrusión a sus sistemas.

La compañía dijo que *hackers* probablemente robaron información en un episodio que **se sospecha ocurrió en agosto de 2013**.

Yahoo dijo que nombres, números de teléfono contraseñas y direcciones de correo electrónico fueron robadas, pero no datos bancarios ni de tarjetas de crédito.

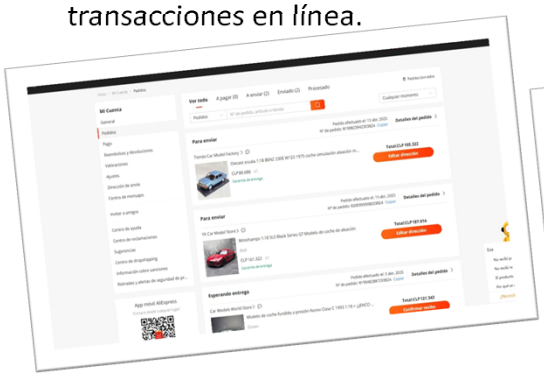
- Yahoo sufre "uno de los mayores ataques informáticos de la historia" con el robo de información de unos 500 millones de cuentas de sus usuarios

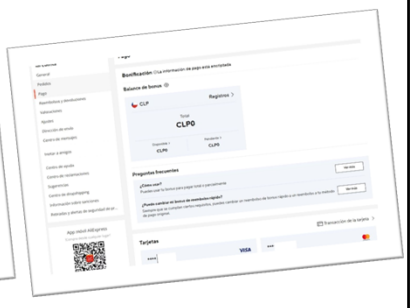
Los usuarios deben cambiar sus contraseñas y preguntas de seguridad como medida de precaución.

Comercio Electronico

Activos de información

- Datos de clientes: Información de pago, historial de compras.
- Plataformas de comercio: Sistemas que gestionan ventas y transacciones en línea.





Comercio Electrónico - Riesgos

- Robo de información de pago: Compromiso de datos de tarjetas de crédito y otras formas de pago.
- Fraude de comercio electrónico: Actividades fraudulentas como compras no autorizadas o falsificación de pedidos.