



Seguridad de la Información y Ciberseguridad

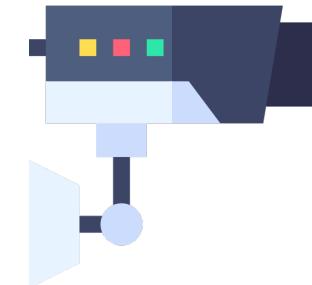
Marco Aravena Vivar

Escuela de Ingeniería Informática, Facultad de Ingeniería
Dirección General de Modernización y Transformación Digital

Seguridad de la información

La Seguridad de la Información, según **ISO27001**, se refiere a la **confidencialidad**, la **integridad** y la **disponibilidad** de la información y los datos importantes para la organización, independientemente del formato que tengan, estos pueden ser:

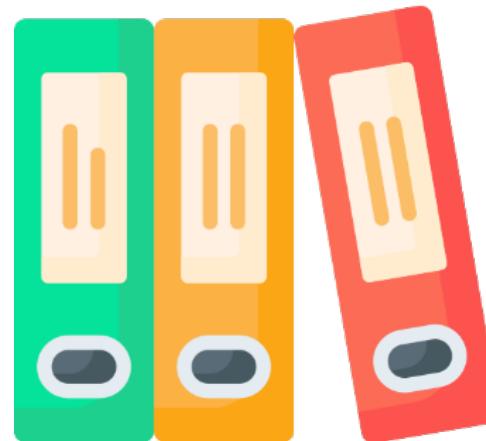
- Electrónicos
- En papel
- Audio y vídeo
- Etc.



Seguridad de la información

Ejemplos:

- Correos electrónicos, se pueden leer??
- Estado de cuenta bancaria.
- Grabaciones de seguridad.
- Cartas.



Seguridad de la información

Seguridad de la Información es el **conjunto de medidas preventivas y reactivas** de las **organizaciones** y sistemas **tecnológicos** que permiten **resguardar y proteger la información**, buscando mantener la **confidencialidad**, la **disponibilidad** e **integridad** de datos.



Seguridad de la información

Los principios básicos o dimensiones de la seguridad de la información son:



Confidencialidad: es la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados.



Integridad: es la propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada.



Disponibilidad: es una característica, calidad o condición de la información que se encuentra a disposición de quien tiene que acceder a esta, bien sean personas, procesos o aplicaciones.

Seguridad de la información y ciberseguridad



La Ciberseguridad se encuentra comprendida dentro de la Seguridad de la Información.

La Ciberseguridad tiene como foco la protección de la información digital que vive en los sistemas interconectados.

Ciberseguridad entonces....

- propone sistemas robustos que sean capaces de actuar antes, durante y después de un incidente.
- correctamente aplicada sirve no solo para prevenir incidentes, sino también dar confianza a los clientes y al mercado, pudiendo así reducir el riesgo de exposición del usuario y de los sistemas.
- desea evitar todo tipo de amenazas, las cuales ponen en riesgo la información que es procesada, transportada y almacenada en cualquier dispositivo.



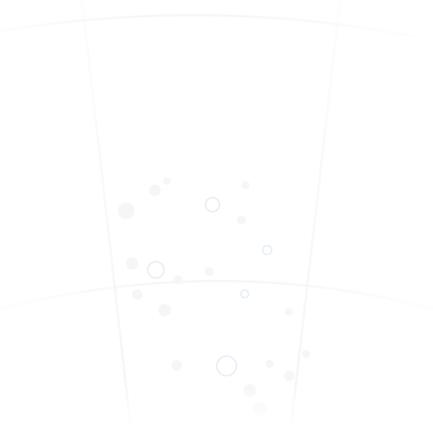
DRP
BCP

ISO 27000
ISO 27001
ISO 27032
ISO 20000



DRP: Disaster Recovery Plan.

BCP: Business Continuity Plan



Marco Aravena Vivar
Escuela de Ingeniería Informática, Facultad de Ingeniería
Dirección General de Modernización y Transformación Digital



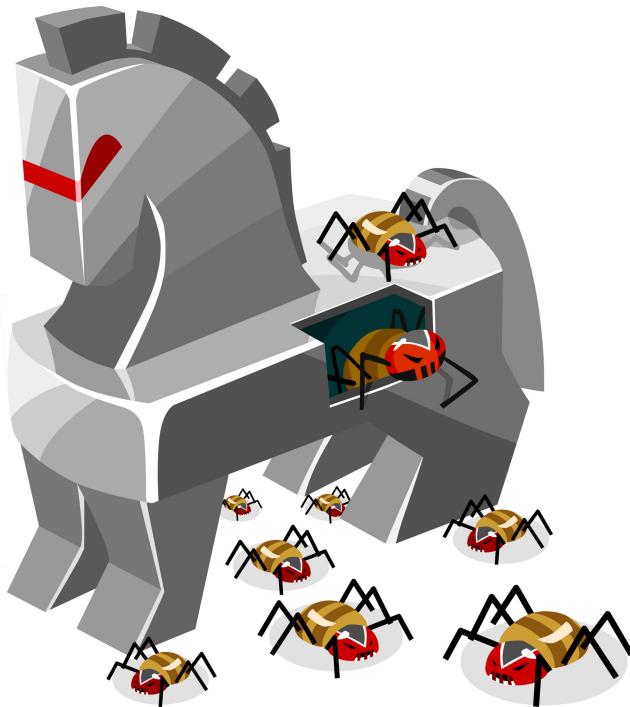
Amenazas

Malware

- Software malicioso es el software que un cibercriminal o un hacker ha creado para interrumpir el funcionamiento o dañar el equipo de un usuario legítimo.
- Es una de las ciberamenazas más comunes.
- Con frecuencia se propaga a través de un archivo adjunto de correo electrónico no solicitado o de una descarga de apariencia legítima.
- Puede ser utilizado por los ciberdelincuentes para ganar dinero o para realizar ciberataques con fines políticos.



Malware: Tipos



- **Virus.** un programa capaz de reproducirse, que se incrusta un archivo limpio y se extiende por todo el sistema informático e infecta a los archivos con código malicio.
- **Troyanos.** un tipo de malware que se disfraza como software legítimo. Los cibercriminales engañan a los usuarios para que carguen troyanos a sus computadoras, donde causan daños o recopilan datos.
- **Spyware.** un programa que registra en secreto lo que hace un usuario para que los cibercriminales puedan hacer uso de esta información. Por ejemplo, el spyware podría capturar los detalles de las tarjetas de crédito.
- **Ransomware.** malware que bloquea los archivos y datos de un usuario, con la amenaza de borrarlos, a menos que se pague un rescate.
- Y muchos más.....

Malware: Ejemplo en Chile

The image shows two web browser windows side-by-side. The left window is from the website [biobiochile.cl](https://biobiochile.cl/noticias/economia/actualidad-economica/2022/08/29/el-sitio-web-y-las-bases-de-datos-del-sernac-ya-llevan-5-dias-secuestreados-por-hackers-solo-la-web-dio-ciertos-guiños). It features a header with the Citroën logo and an advertisement for the Citroën SpaceTourer car. The main content discusses the hacking of the Sernac website, mentioning it has been compromised for 5 days and only the website itself was affected. The right window is from the website [csirt.gob.cl](https://csirt.gob.cl/noticias/alerta-de-seguridad-cibernetica-incidente-en-servicio-publico), specifically the 'Alerta de Seguridad Cibernetica' section. It highlights a cyber attack on a public service, mentioning ransomware and encrypted files. Both pages include social media sharing options and navigation menus.

Bases de datos de Sernac cumplieron 5 días secuestrados por hackers: sólo la web dio ciertos guiños

Por Verónica Reyes

Lunes 29 agosto de 2022 | 10:09

SERNAC
Servicio Nacional del Consumidor

Agencia UNO 70,792 visitas

ALERTA DE SEGURIDAD CIBERNÉTICA: INCIDENTE EN SERVICIO PÚBLICO

El Equipo de Respuesta ante Incidentes de Seguridad Informática, **CSIRT de Gobierno**, informa sobre un incidente en progreso que afecta a un servicio del gobierno, durante la jornada del jueves 25 de agosto, el cual ha interrumpido el funcionamiento de sus sistemas y servicios en línea.

La naturaleza del incidente corresponde a un ransomware que afectó servidores Microsoft y VMware ESXi en redes corporativas de la institución.

El ransomware en cuestión tiene la capacidad de detener todas las máquinas virtuales en ejecución y cifrar archivos relacionados con las máquinas virtuales.

Como resultado de la infección, los archivos asumen la extensión ".crypt". Posteriormente, el atacante toma control completo del sistema de la víctima y deja un mensaje de rescate informando la cantidad de datos secuestrados, ofreciendo un canal de comunicación y un ID específico para contactarse con ellos. El atacante da un plazo de tres días para comunicarse, de lo contrario amenaza con impedir que los datos sean accesibles para la organización y poner estos activos a la venta a terceros en la darkweb.

El ransomware utilizaría el algoritmo de cifrado de clave pública NTRUEncrypt, dirigido a archivos de registro (.log), archivos ejecutables (.exe), archivos de bibliotecas dinámicas

Malware: Ejemplo en Chile

biobiochile.cl



Economía

Plataforma web de Mercado Público proveedor tecnológico sufrió ciberataque

Por Verónica Reyes

Jueves 14 septiembre de 2023 | 13:25



© Pixabay

La empresa IFX Networks, que es quien provee servicios a Mercado Público, sufrió un evento de ransomware. Se entregaron los lineamientos para proceder en los procesos de compra mientras dure esta contingencia.

Universidad
de Valparaíso
CHILE

biobiochile.cl

biobiochile.cl

Economía

Portal Mercado Público se recupera tras ciberataque que lo dejó con problemas

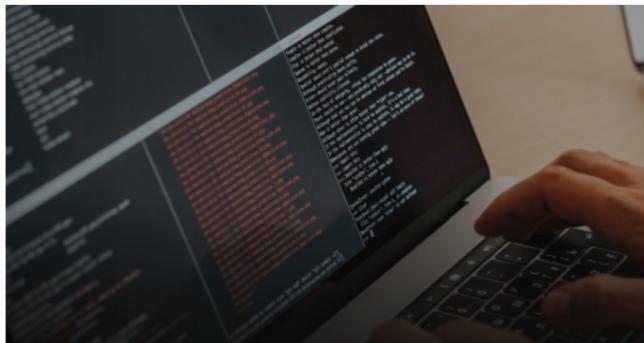
Por Fernanda Pino

Martes 03 octubre de 2023 | 19:02

Ingresa a Comunidad Bio Bío



Leer más tarde



Contexto | ChileCompra

2,144 visitas

Chile Compra y Mercado Público habilitan sus sitios web luego de estar 20 días con sus servicios caídos tras un ciberataque por un grupo de hackers que se hacen llamar RansomHouse, quienes intervinieron los servidores con un virus llamado "Mario Locker". Este virus fue catalogado como uno de los más grandes



"Es un honor": Espacio Food & Service convirtió a Santiago en

HASTA MARZO DE 2029

Comisión Nacional de Acreditación CNA-Chile



Hackers, Hacking y Ética.

Marco Aravena Vivar

Escuela de Ingeniería Informática, Facultad de Ingeniería
Dirección General de Modernización y Transformación Digital

¿Qué es hacking?

- El hacking se puede definir como la búsqueda y explotación de vulnerabilidades de seguridad en sistemas o redes.
- Requiere de conocimientos y habilidades para ejecutar una metodología de detección y explotación de vulnerabilidades.



Activo....vulnerabilidad.....amenaza ?????

Familia, muebles,
equipos
(Activos)

Techo roto
(Vulnerabilidad)

Lluvia
(Amenaza)



Habilidades para el Hacking:

- Habilidades necesarias para incursionar el Hacking Ético y Ciberseguridad:
 - Configuración y uso de máquinas virtuales.
 - Uso de línea de comandos (shell).
 - Administración de Sistemas.
 - Gestión y Análisis de Redes de Computadores



Tipos de hackers



	White Hat	Black Hat	Grey Hat
Fines Maliciosos	No	Si	No
Contratado por empresa	Si	No	No
Con permiso	Si	No	No

¿Qué es el Hacking Ético?



- Es una forma para referirse al acto de un **hacker** que utiliza sus **conocimientos de informática y seguridad** para **encontrar vulnerabilidades o fallas de seguridad en el sistema**, con el objetivo de reportarlas en la organización para que se **tomen todas las medidas necesarias**.
- Los profesionales que se dedican al Hacking Ético, **practican una serie de pruebas**, cuyo **objetivo** es **poder burlar la seguridad** que el **servicio/red**, con la única intención de **probar su efectividad**, o por el contrario, **demostrar la vulnerabilidad** de un sistema.

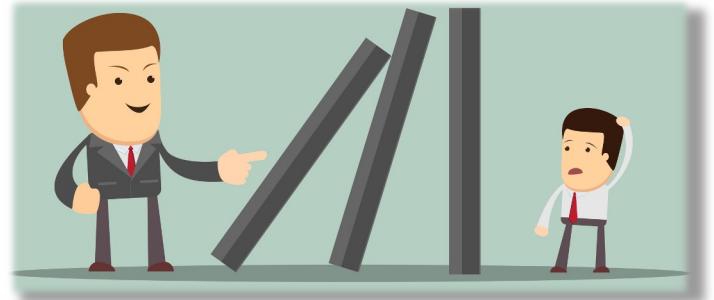
¿Por qué Ético?

- Para poder emular un ataque y que este no cause daño tiene que haber una ética.
- Ejemplo de simulación al robo de un banco:
 - Sin armas.
 - Se prueba la eficiencia de la seguridad.
 - Se informa como se hizo y lo que se debe de mejorar.
- La ética implica que el trabajo y la intervención del profesional **no compromete** a la organización.



¿Por qué Ético?

- Se pueden generar diferentes daños:
 - Alteración: Modificar registros o datos
 - Borrado: Destruir información o sobrescribir
 - Filtración: Incumplimiento normas de confiabilidad
 - Sustracción: Robar o guardar datos en otros medios
- También, se puede producir daño con la divulgación, como ver, hablar, escuchar y manipular los resultados mientras se hacen los análisis.



¿Por qué Ético?

- Conductas mínimas que debe de tener un profesional.
 - Hacer su trabajo de la mejor manera posible.
 - Dar el mejor reporte.
 - Respetar el secreto.
 - No hablar mal ni inculpar a un administrador o equipo de programadores.
 - No aceptar sobornos.



¿Por qué Ético?

- Conductas mínimas que debe de tener un profesional.
 - No manipular o alterar resultados o análisis.
 - Delegar tareas específicas en alguien más capacitado.
 - No prometer algo imposible de cumplir.
 - Ser responsable en su rol y función.
 - Manejar los recursos de modo eficiente.



La ética no es trivial de determinar...

The screenshot shows a news article from the website www.debate.com.mx/viral/Nicolas-Maduro-bloquea-a-Elon-Musk-en-X-. The article is titled "Nicolás Maduro bloquea a Elon Musk en X, pero el dueño de la red social se desbloquea a sí mismo". The page includes a sidebar with social media sharing icons (Messenger, Facebook, WhatsApp, Email, Telegram, Instagram, X) and a sidebar for Hawaiian Airlines with a bonus offer.

Nicolás Maduro bloquea a Elon Musk en X, pero el dueño de la red social se desbloquea a sí mismo

Por medio de X (antes Twitter), el conflicto del reelecto presidente de Venezuela, Nicolás Maduro y el empresario multimillonario, Elon Musk, generó una ola de reacciones.

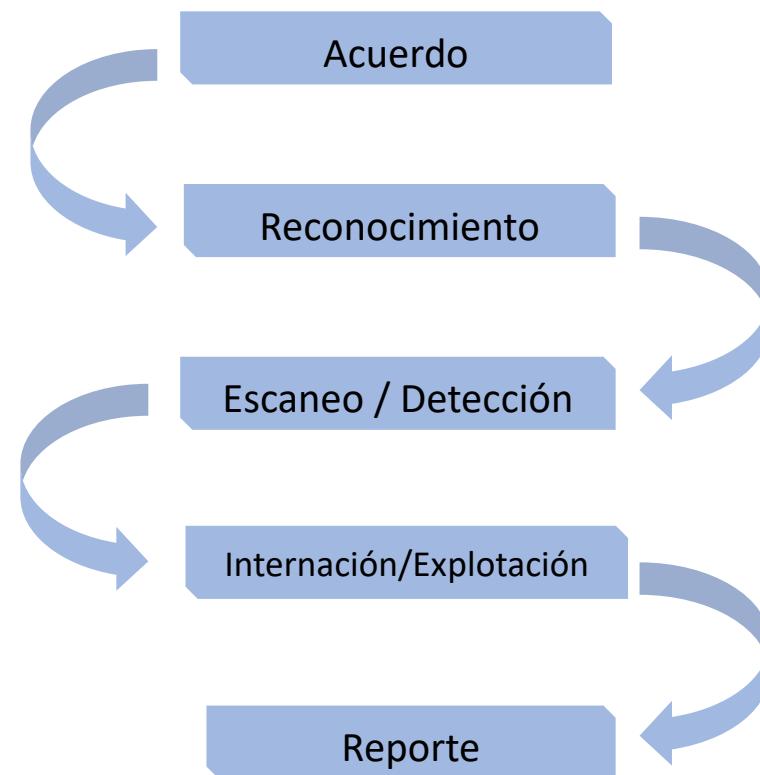


Metodología de Hacking Ético.

Marco Aravena Vivar

Escuela de Ingeniería Informática, Facultad de Ingeniería
Dirección General de Modernización y Transformación Digital

Metodología de Hacking Ético



Metodología de Hacking Ético

Acuerdo

Reconocimiento

Escaneo / Detección

Internación/Explotación

Reporte



1. Acuerdo Se establece los límites y las pruebas que se van a aplicar, de una manera de mantener un control sobre el espacio y los datos. Se debe de declarar con detalle lo que se va a realizar y a lo que se quiere llegar.

The screenshot shows a digital interface for managing legal documents. At the top, it lists several laws: LEY 19223 (Tipificación de figuras penales relativas a la Informática), LEY 21459 (Establece normas sobre delitos informáticos, deroga la Ley N° 19.223 y modifica otros cueros legales con el objeto de adecuarlos al Convenio de I), LEY 21663 (Ley Marco de Ciberseguridad), and LEY 2024 (Promulgación: 26-MAR-2024, Publicación: 08-ABR-2024). The interface includes a search bar, download links, and social media sharing buttons. A large central area displays a handshake icon, likely representing the 'Acuerdo' (Agreement) step in the methodology.

Metodología de Hacking Ético

Acuerdo

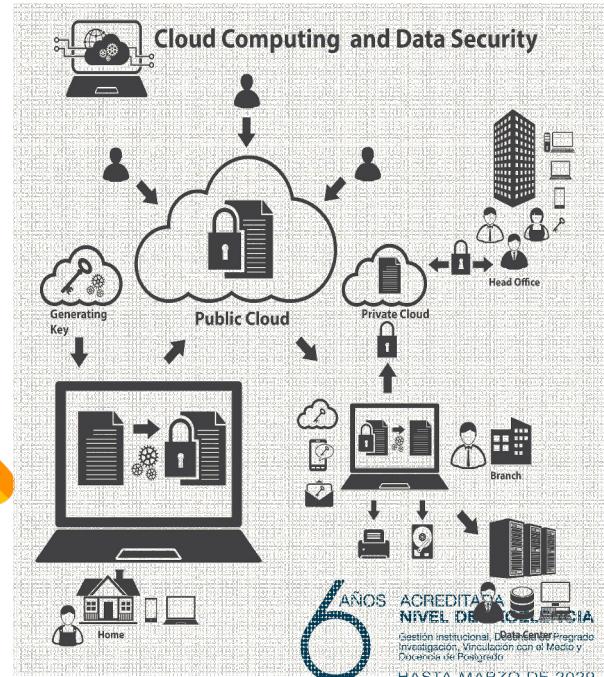
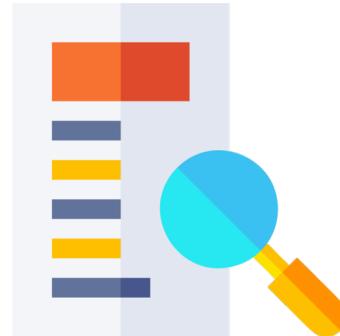
Reconocimiento

Escaneo / Detección

Internación/Explotación

Reporte

2. Reconocimiento El hacker emplea todo lo que tiene para poder obtener información sobre el medio que va a atacar.



Metodología de Hacking Ético

Acuerdo

Reconocimiento

Escaneo / Detección

Internación/Explotación

Reporte

3. Escaneo/Detección se utilizan herramientas y técnicas para escanear la red y los sistemas en busca de posibles vulnerabilidades. Estas herramientas identifican puertos abiertos, servicios en ejecución y posibles debilidades que podrían ser explotadas más adelante.



Metodología de Hacking Ético

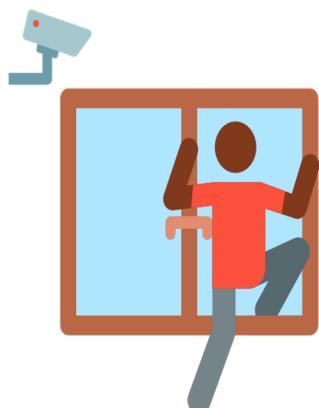
Acuerdo

Reconocimiento

Escaneo / Detección

Internación/Explotación

Reporte



4. Internación/Explotación Una vez identificadas las vulnerabilidades, se intenta aprovecharlas para ganar acceso a los sistemas objetivo, por ejemplo, explotación de debilidades en aplicaciones, configuraciones inseguras o técnicas de ingeniería social para obtener credenciales de acceso legítimas.

Metodología de Hacking Ético

Acuerdo

Reconocimiento

Escaneo / Detección

Internación/Explotación

Reporte

5. Reporte Una vez finalizado todo el ataque se recopila la información obtenida y se diseña un reporte con las conclusiones sobre el ataque, indicando las vulnerabilidades, métodos y sugerencias.

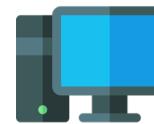
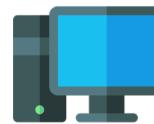
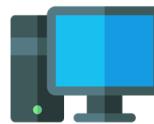


Resumen Metodología de Hacking Ético

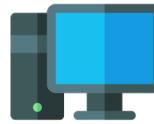
Acuerdo



Reconocimiento



Escaneo / Detección



Internación/Explotación



MySQL

FTP

Reporte



AÑOS ACREDITADA
NIVEL DE EXCELENCIA
Gestión Institucional, Docencia de Pregrado
Investigación, Vinculación con el Medio y
Docencia de Postgrado
HASTA MARZO DE 2029



Veamos un ejemplo.....

- Escenario y actividades:
 - Se ha llegado al acuerdo de analizar las vulnerabilidades de un servidor Linux con IP conocida (reconocimiento realizado).
 - Se realizará un escaneo para detectar vulnerabilidades.
 - Si existen vulnerabilidades se intentará explotarlas.
 - Posibles recomendaciones.

Veamos un ejemplo.....

Atacante(Kali Linux)

Víctima (Linux)



Marco Aravena Vivar
Escuela de Ingeniería Informática, Facultad de Ingeniería
Dirección General de Modernización y Transformación Digital



Conclusiones

Conclusiones.



- La ciberseguridad es un tema contingente y relevante que requiere concientización y capacitación.
- Hacking Ético y Ciberseguridad requiere habilidades + conocimientos + ética.
- Hacking Ético es una medida de protección ante la ciberdelincuencia:
 - Metodología simple pero muy efectiva.
 - Permite detectar vulnerabilidades y proponer mejoras.
 - La ética como pilar.



Seguridad de la Información y Ciberseguridad

Escuela de Ingeniería Informática, Facultad de Ingeniería
Dirección General de Modernización y Transformación Digital