APUNTES DEL MÓDULO 1

Amenazas digitales y seguridad de la información

Ciber Higiene y Buenas Prácticas de Seguridad de la Información para Usuarios

Material de estudio

Módulo 1

Apunte descargable del estudiante

Contenido del módulo

1. **El Fundamento: Ciberseguridad, Ciberhigiene y el Marco Legal Chileno**
2. **Identificando las Amenazas Digitales Más Comunes**
3. **Anatomía de un Incidente Informático y sus Consecuencias**
4. **Los Tres Pilares de la Seguridad de la Información: Confidencialidad, Integridad y Disponibilidad (CIA)**
5. **Activos de Información y Riesgos Asociados**
6. **Tu Rol Esencial: Reporte y Acción en la Gestión de Incidentes**

¡Hola! Te doy la bienvenida a este módulo fundamental sobre Ciberhigiene y Buenas Prácticas de Seguridad de la Información. En un mundo cada vez más digitalizado, comprender las amenazas y cómo proteger nuestra información es crucial, tanto en nuestra vida personal como en el ámbito laboral. Este módulo te proporcionará las herramientas necesarias para identificar los peligros digitales más comunes y entender los pilares esenciales de la seguridad de la información: confidencialidad, integridad y disponibilidad. A través de casos y ejemplos concretos, aprenderás a aplicar estos conocimientos en tu día a día, convirtiéndote en una pieza clave para la protección de nuestra organización.

1 El Fundamento: Ciberseguridad, Ciberhigiene y el Marco Legal Chileno

La **ciberseguridad** no es solo un dominio de expertos en TI; es una responsabilidad compartida que nos concierne a todos. Se define como la protección de sistemas, redes y programas frente a ataques digitales cuyo objetivo es acceder, modificar o destruir información sensible. Por otro lado, la **ciberhigiene** se refiere al conjunto de prácticas sencillas y rutinarias que cada usuario debe adoptar para mantener la seguridad de la información. Piensa en ella como la higiene personal aplicada al mundo digital: así como lavarse las manos previene enfermedades, las acciones de ciberhigiene previenen incidentes de seguridad.

En Chile, el marco legal que rige la ciberseguridad se ha fortalecido significativamente. La **Ley N°21.663, Ley Marco de Ciberseguridad**, estableció la Agencia Nacional de Ciberseguridad (ANCI) y el CSIRT Nacional para coordinar la prevención y respuesta a incidentes. Esta ley impone a muchas organizaciones el deber legal de reportar incidentes significativos, lo que subraya la importancia de tu reporte interno ante cualquier sospecha. Adicionalmente, la futura **Ley N°21.719 de Protección de Datos Personales**, que entrará en vigencia en diciembre de 2026, refuerza la necesidad de proteger la información personal que manejamos, tanto de clientes como de colegas, dotando de mayores derechos a los titulares de los datos y de mayores responsabilidades a quienes los procesan.



La ciberseguridad es una responsabilidad compartida: todos debemos estar atentos y ser parte de la solución.

✔ Puntos clave

- La ciberseguridad es una responsabilidad compartida, no solo de TI.
- La ciberhigiene son prácticas rutinarias que cualquier usuario puede implementar.
- La Ley N°21.663 fortalece la respuesta nacional a incidentes y obliga al reporte.
- La futura Ley N°21.719 aumenta la protección de datos personales y las responsabilidades corporativas.

💭 Para reflexionar

- ¿Cómo se diferencia la ciberhigiene de la ciberseguridad en tus tareas diarias?
- ¿Por qué es importante para ti como usuario conocer el marco legal chileno de ciberseguridad?
- ¿Qué implicaciones tiene para tu trabajo la próxima Ley de Protección de Datos Personales?

2 Identificando las Amenazas Digitales Más Comunes

Para proteger la información eficazmente, es fundamental conocer las amenazas digitales más comunes. Saber identificarlas es la primera línea de defensa, ya que todos estamos expuestos a estos riesgos en el entorno digital. Las amenazas digitales son incidentes que pueden comprometer la seguridad de la información.

- **Malware:** Es un término genérico para software malicioso (virus, troyanos, spyware, gusanos) diseñado para dañar un equipo, tomar su control o robar información.
- **Phishing:** Técnica de ingeniería social que suplanta la identidad de una entidad de confianza (banco, jefe, servicio de entrega) para engañar al usuario y que este revele credenciales, haga clic en enlaces maliciosos o descargue archivos infectados. Sus variantes son:
  - **Vishing:** Phishing realizado a través de llamadas de voz.
  - **Smishing:** Phishing a través de mensajes SMS.
  - **Spear Phishing:** Phishing altamente dirigido y personalizado a una persona o grupo específico dentro de una organización.
- **Ransomware:** Tipo de malware que cifra los archivos de un sistema, dejándolos inaccesibles, y luego exige un rescate (generalmente en criptomonedas) para restaurar el acceso. La mejor defensa son los respaldos de información actualizados.
- **Filtración de Información (Data Breach):** Ocurre cuando información confidencial o datos personales son expuestos, accedidos o robados sin autorización. Esto puede tener graves consecuencias legales y reputacionales para la organización, así como para las personas cuyos datos son afectados.
- **Ingeniería Social:** Manipulación psicológica de personas para que realicen acciones o divulguen información confidencial. Se aprovecha de emociones como la urgencia, la autoridad, el miedo o la curiosidad. El atacado directo aquí es el ser humano, no la máquina.

✔ Puntos clave

- Malware abarca virus, troyanos y spyware que dañan sistemas o roban datos.
- Phishing (incluyendo vishing, smishing y spear phishing) utiliza engaños para obtener información sensible.
- Ransomware cifra archivos y exige rescate; los respaldos son la mejor protección.
- Las filtraciones de datos exponen información confidencial con graves consecuencias.
- La ingeniería social manipula psicológicamente a las personas para explotar la seguridad.

💭 Para reflexionar

- ¿Puedes recordar algún correo sospechoso que hayas recibido? ¿Cómo aplicaría el concepto de phishing?
- Si tuvieras un ransomware en tu equipo, ¿qué sería lo primero que notarías?
- ¿Cómo podrías identificar un intento de ingeniería social en una llamada telefónica en tu trabajo?

3 Anatomía de un Incidente Informático y sus Consecuencias

Los incidentes informáticos rara vez son aleatorios; suelen ser el resultado de un vector de ataque que explota una vulnerabilidad, a menudo humana. Entender cómo se desarrollan te ayudará a estar más alerta.

Los **vectores de ataque** son los caminos o métodos que los ciberdelincuentes utilizan para acceder a sistemas o información. Algunos de los más comunes incluyen:

- **Correos electrónicos de phishing:** Contienen enlaces o adjuntos maliciosos que, al ser abiertos, instalan malware o redirigen a sitios fraudulentos.
- **Sitios web comprometidos:** Sitios legítimos que han sido alterados para descargar malware automáticamente (*drive-by download*) o solicitar credenciales.
- **Dispositivos USB infectados:** Pueden introducir malware al conectarse a un equipo, especialmente si el software de seguridad no está actualizado.
- **Redes Wi-Fi inseguras:** Redes públicas o mal configuradas que permiten la intercepción de información por parte de atacantes.
- **Contraseñas débiles o reutilizadas:** Facilitan el acceso no autorizado a múltiples servicios si una contraseña es comprometida en un solo sitio.

Las **consecuencias para la persona** pueden ser graves: robo de identidad, pérdida de datos personales (fotos, documentos), interrupción del trabajo e incluso problemas legales si se compromete información confidencial de la empresa. Para la **organización**, las consecuencias son aún más amplias:

- Pérdidas económicas directas (rescates de ransomware, costos de recuperación).
- Interrupción de servicios críticos que afecta la operación diaria.
- Daño severo a la reputación y pérdida de la confianza de clientes y socios.
- Multas y sanciones por incumplimiento normativo (Ley N°21.663, futura Ley N°21.719).
- Pérdida de propiedad intelectual o secretos comerciales.

Tu reporte rápido y efectivo de cualquier sospecha es crucial para mitigar el impacto, considerando que en Chile muchas organizaciones tienen el deber legal de reportar incidentes significativos a las autoridades.



Tu reporte oportuno ante cualquier sospecha es la primera línea de defensa contra las amenazas digitales.

✔ Puntos clave

- Los incidentes informáticos son causados por vectores de ataque que explotan vulnerabilidades.
- Vectores comunes incluyen phishing, sitios web comprometidos, USBs infectados y contraseñas débiles.
- Las consecuencias para individuos incluyen robo de identidad y pérdida de datos personales.
- Para la organización, las consecuencias son pérdidas económicas, daño reputacional y multas legales.
- El reporte temprano de un incidente es vital para mitigar el daño y cumplir con la normativa.

💭 Para reflexionar

- ¿Qué tipo de información personal podría verse afectada si tu laptop de trabajo fuera robada?
- Si descubres un dispositivo USB desconocido conectado a tu equipo, ¿cuál sería el riesgo potencial?
- ¿Cómo podría un incidente informático afectar la reputación de nuestra organización ante los clientes?

4 Los Tres Pilares de la Seguridad de la Información: Confidencialidad, Integridad y Disponibilidad (CIA)

Para proteger la información de manera efectiva, es vital comprender los tres principios fundamentales de la seguridad de la información, conocidos como la tríada CIA. Estos pilares guían todas nuestras acciones de ciberseguridad y son interdependientes; si uno falla, los otros también pueden verse afectados.

Principio CIA	Descripción	Aplicación en el Trabajo
Confidencialidad	Asegura que la información solo sea accesible y visible para las personas o entidades autorizadas.	No compartir contraseñas, usar bloqueo de pantalla al ausentarse, restringir acceso a archivos a quienes lo necesitan, evitar dejar documentos sensibles a la vista.
Integridad	Garantiza que la información sea precisa, completa y no haya sido alterada o destruida sin autorización, ya sea accidental o intencionalmente.	Proteger archivos de manipulación por malware, asegurar que los datos no se corrompan durante la transmisión, usar copias de seguridad para restaurar versiones correctas si hay errores.
Disponibilidad	Se refiere a que la información debe estar accesible y utilizable cuando sea requerida por los usuarios autorizados, en el momento que la necesiten.	Realizar respaldos periódicos de información crítica para recuperarla ante un ataque de ransomware o falla del sistema, asegurar que los sistemas estén operativos y accesibles, mantener la infraestructura de red funcionando.

Consideremos un ejemplo práctico: un contrato de un cliente. Su **confidencialidad** se asegura al limitar su acceso solo a los abogados y gerentes involucrados. Su **integridad** se garantiza con firmas digitales y versiones controladas que impiden modificaciones no autorizadas. Finalmente, su **disponibilidad** se asegura mediante el almacenamiento en un servidor con respaldo, accesible siempre que se necesite para una consulta legal.

✔ Puntos clave

- La Confidencialidad asegura que solo usuarios autorizados accedan a la información.
- La Integridad garantiza que la información sea precisa, completa y no modificada sin permiso.
- La Disponibilidad asegura que la información esté accesible y utilizable cuando se necesite.
- Estos tres principios son interdependientes y forman la base de una estrategia de seguridad robusta.

💭 **Para reflexionar**

- Si tuvieras un documento confidencial en tu escritorio y te ausentas, ¿qué principio de seguridad se vería comprometido si lo dejas abierto?
- ¿Qué harías para garantizar la integridad de un informe financiero antes de enviarlo por correo?
- ¿Cómo afecta la disponibilidad de un sistema si hay una falla de energía prolongada en la oficina?

5 Activos de Información y Riesgos Asociados

Ahora que hemos cubierto los principios de seguridad, es clave identificar qué estamos protegiendo. Un **activo de información** es cualquier elemento de valor para la organización que contiene o procesa información. Esto incluye no solo los datos en sí, sino también los sistemas, el hardware, el software y las personas que interactúan con ellos.

Ejemplos de activos de información en tu día a día laboral:

- **Datos:** Bases de datos de clientes, contratos, información financiera, planos de proyectos, informes internos, historiales de pacientes, etc.
- **Hardware:** Tu computador de escritorio, laptop, smartphone corporativo, servidores, impresoras, dispositivos de red.
- **Software:** Sistemas operativos, aplicaciones de oficina (Microsoft 365, Google Workspace), programas especializados (CRM, ERP), sistemas de gestión de proyectos.
- **Documentos físicos:** Archivos en papel, expedientes de clientes, contratos impresos.
- **Personas:** Tú y tus compañeros, quienes tienen acceso, conocimiento y la capacidad de procesar información.

Para cada activo, existen **riesgos**: eventos o circunstancias que podrían causar daño a la confidencialidad, integridad o disponibilidad de la información. Reconocerlos nos permite aplicar las medidas correctas y entender la importancia de cada acción de ciberhigiene.

Activo de Información	Ejemplo de Riesgo	Principio Afectado
Base de datos de clientes	Acceso no autorizado por un ciberatacante	Confidencialidad
Contrato digital	Modificación accidental o intencionada sin control	Integridad
Servidor de archivos	Falla de hardware que impide el acceso a documentos	Disponibilidad
Laptop corporativa	Pérdida o robo del dispositivo	Confidencialidad, Disponibilidad
Correo electrónico	Phishing que lleva a la filtración de credenciales	Confidencialidad
Documentos físicos	Incendio o inundación de la oficina	Disponibilidad, Integridad
Sistema ERP	Vulnerabilidad de software que permite inyección de código	Integridad, Confidencialidad

Comprender estos riesgos te permite actuar de forma preventiva, saber qué reportar en caso de sospecha y valorar la importancia de cada práctica de seguridad.

✔ Puntos clave

- Los activos de información incluyen datos, hardware, software, documentos físicos y personas.
- Los riesgos son eventos que pueden dañar la confidencialidad, integridad o disponibilidad de los activos.
- La identificación de riesgos permite aplicar medidas preventivas adecuadas.
- Cada tipo de activo de información tiene riesgos específicos asociados que deben ser gestionados.

💭 Para reflexionar

- ¿Qué activos de información manejas diariamente en tu puesto de trabajo?
- Si tuvieras un problema con el sistema de gestión de clientes, ¿qué principios de la seguridad de la información podrían verse afectados?
- ¿Qué riesgo de seguridad identificarías si dejara un documento físico confidencial en la impresora sin recogerlo?

6 Tu Rol Esencial: Reporte y Acción en la Gestión de Incidentes

Hemos visto las amenazas y la importancia de proteger nuestros activos. Ahora, cerramos este módulo reforzando tu papel esencial en la gestión de incidentes. En el ciclo de la seguridad de la información, el usuario final es un pilar fundamental. Aunque tu rol no es resolver un incidente complejo, tu capacidad para detectarlo y reportarlo rápidamente es la clave para minimizar su impacto y cumplir con las normativas.

¿Por qué es crucial tu reporte?

- **Mitigación temprana:** Un reporte inmediato permite que el equipo de TI actúe antes de que el incidente escale, conteniendo el daño a tiempo.
- **Cumplimiento legal:** Como se mencionó, la Ley N°21.663 exige a muchas organizaciones el reporte de incidentes significativos. Tu aviso interno es el primer paso para cumplir con esta obligación legal.
- **Protección de datos:** La pronta detección ayuda a proteger los datos personales y confidenciales, evitando filtraciones que pueden acarrear multas y pérdida de confianza.
- **Aprendizaje y mejora:** Cada incidente reportado, incluso los falsos positivos, proporciona información valiosa para mejorar nuestras defensas y procedimientos de seguridad.

¿Qué debes reportar y cómo?

- Cualquier actividad inusual: Correos sospechosos, ventanas emergentes extrañas, rendimiento lento del equipo sin razón, archivos inaccesibles.
- Pérdida o robo de dispositivos: Tu laptop o smartphone corporativo.
- Errores en la seguridad: Contraseñas expuestas, acceso a información no autorizada.
- Incidentes de ingeniería social: Intentos de engaño por teléfono o presencial.

El procedimiento es sencillo: **ante cualquier sospecha, no intentes resolverlo por tu cuenta.** Contacta inmediatamente al área de TI o al canal de reporte de seguridad establecido en tu organización. Sé lo más preciso posible al describir lo sucedido. Tu proactividad es nuestro escudo más fuerte.

✔ Puntos clave

- El usuario final es fundamental en la detección y reporte de incidentes.
- El reporte temprano permite la mitigación del daño y el cumplimiento legal.
- El reporte protege datos y ayuda a mejorar las defensas de la organización.
- Reporta cualquier actividad inusual, pérdida de dispositivos, errores de seguridad o intentos de ingeniería social.
- No intentes resolver incidentes por tu cuenta; contacta siempre al equipo de TI.

💭 **Para reflexionar**

- ¿Cuál sería el primer paso que tomarías si sospecharas de un intento de phishing en tu correo electrónico?
- ¿Por qué es importante no intentar 'arreglar' un posible problema de seguridad por tu cuenta?
- ¿Cómo crees que un reporte oportuno beneficia a toda la organización, no solo a ti?

🗺 Esquema del Módulo: Amenazas Digitales y Seguridad de la Información

Introducción a la Ciberhigiene	Comprender la ciberseguridad como responsabilidad compartida y la importancia de la ciberhigiene, junto con el marco legal chileno (Ley N°21.663 y futura Ley N°21.719).
Amenazas Digitales Comunes	Identificar malware (virus, ransomware), phishing (vishing, smishing, spear phishing), filtración de información e ingeniería social.
Anatomía de Incidentes Informáticos	Conocer los vectores de ataque y las graves consecuencias de los incidentes para individuos y organizaciones.
Pilares de la Seguridad: CIA	Entender la Confidencialidad, Integridad y Disponibilidad como principios fundamentales para la protección de la información.
Activos de Información y Riesgos	Identificar los activos de información en el ámbito laboral y los riesgos específicos que afectan a cada uno, vinculándolos con la tríada CIA.
Tu Rol en el Reporte de Incidentes	Reconocer la importancia crítica del reporte rápido de incidentes para la mitigación, cumplimiento legal y mejora continua de la seguridad.

En síntesis. Hemos llegado al final de este módulo. Espero que ahora tengas una comprensión sólida de las amenazas digitales y los principios fundamentales de seguridad de la información. Recuerda, tu rol es invaluable. Al aplicar la ciberhigiene en tu día a día y reportar cualquier incidente o sospecha, no solo te proteges a ti mismo, sino que también contribuyes a la seguridad y el bienestar de toda nuestra organización. ¡Mantente alerta y sigue aplicando estas buenas prácticas!