



FUNDAMENTOS DE SEGURIDAD DE LA INFORMACIÓN

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



Manuel Rojas V
Ingeniero en Informática
Magister en Tecnologías de Información

Fundamentos de Seguridad de la Información

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



1 . Seguridad de la información. | Horas de la Unidad: 16 | Horas Presenciales: 16 | Horas Online: 0

APRENDIZAJES ESPERADOS	CRITERIOS DE EVALUACIÓN	CONTENIDOS MÍNIMOS OBLIGATORIOS
1.1 Aplica los elementos que conforman la Triada de la seguridad de la información, para dar cumplimiento a las normas y procedimientos establecidos en el marco de los Framework de seguridad.	<p>1.1.1 Explica los fundamentos de la seguridad de la información, en base a la triada de la seguridad de la información.</p> <p>1.1.2 Identifica las diferencias entre seguridad de la información y seguridad informática, acorde con definiciones de los framework y estándares de la industria.</p> <p>1.1.3 Describe los requisitos para la implementación de un sistema de gestión de la seguridad de la información, acorde con la ISO 27001.</p> <p>1.1.4 Selecciona controles de seguridad que se deben aplicar a una problemática, de acuerdo con definiciones de CIS Controls.</p>	<ul style="list-style-type: none"> Fundamentos de la seguridad de la información. Objetivos de la seguridad de la información. Seguridad informática. Framework de seguridad: ISO 27001:2022 CIS Controls.

Agenda

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



Seguridad de la información

- Confidencialidad
- Integridad
- Disponibilidad (CIA).

Orígenes y Tipos de Atacantes.

Mecanismos de Seguridad Pasiva y Activa.

Normativa.

- ISO 27000.
- ISO 27001.
- ISO 27002.

NIST Cybersecurity Framework.

Criptografía simétrica y asimétrica.

Tipos de Cifrado:

- DES,
- 3DES,
- AES,
- RSA,
- Blowfish,
- Twofish.

*“Si te conoces a ti mismo y conoces a tu enemigo, entonces no
deberás temer el resultado de mil batallas”*

- Sun-Tzu,
- El Arte de la Guerra




¿De dónde surge la seguridad?



“Tecnológicamente, la seguridad es GRATIS”

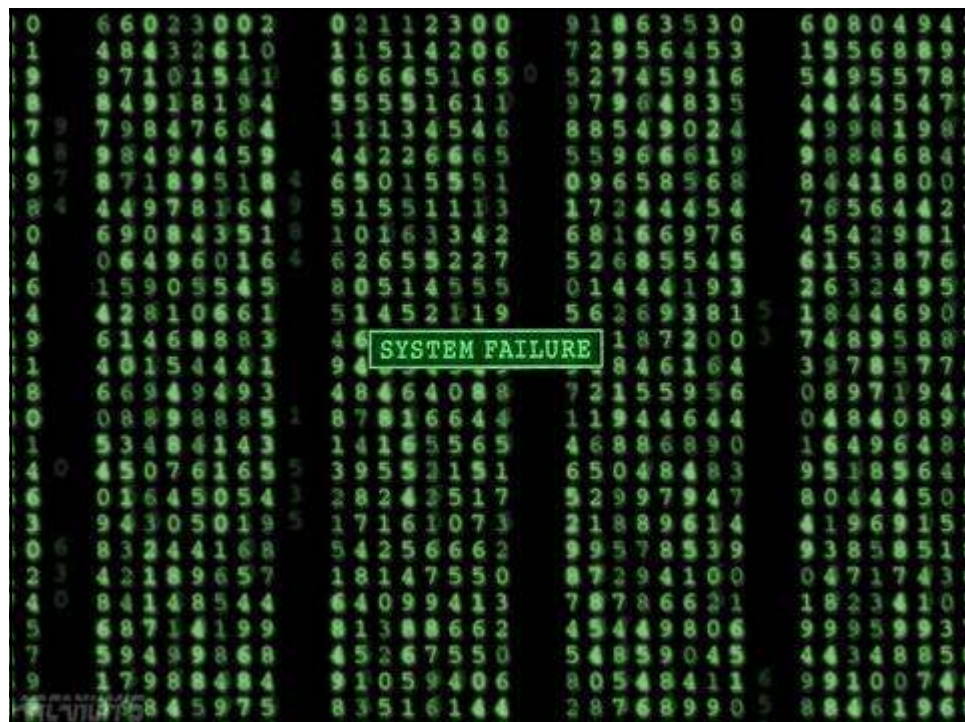
YA HAS PAGADO POR ELLA: Los sistemas operativos modernos
contienen muchas características de seguridad. ¿Las
conoces? ¿Las usas?

LAS MEJORES HERRAMIENTAS DE SEGURIDAD SON OPEN
SOURCE. (excepto los antivirus)

¿De dónde surge la seguridad?

 La Seguridad Informática es Fácil: “Con el 20% de esfuerzo
se puede lograr el 80% de resultados”

-  Actividades sencillas pero constantes son las que evitan la mayoría de los problemas.
-  Se debe de trabajar en crear **MECANISMOS** de seguridad que usan las **TECNICAS** de seguridad adecuadas según lo que se quiera proteger.





¿Qué es la información?

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



La **información** es un bien que, como otros bienes importantes de la organización, tiene valor y requiere ser adecuadamente protegido



La información se puede presentar:

Impresa o escrita en papel
Almacenada electrónicamente
Transmitida por correo u otros medios electrónicos
Mostrada en videos corporativos
En conversaciones

Seguridad de la Información

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- La seguridad
 - Es una primera barrera de entrada psicológica y real para el modelo de negocios basado en la red.
 - Es percibida como uno de los atributos importantes del servicio.
- Las redes en sí son un medio inseguro, pero correctamente administradas pueden convertirse en un canal seguro.
- Es obligación de las empresas adoptar medidas de seguridad efectivas.
- La seguridad debe ser un compromiso real de la alta gerencia.

Seguridad de la Información

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- La Seguridad de la Información:
 - Problema de negocio, no tecnológico
 - Sólo controles tecnológicos = **FRACASO**.
 - La tecnología de seguridad, por si sola, no puede eliminar todos los peligros potenciales

Seguridad de la Información

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- Necesidad de un modelo que unifique las medidas tecnológicas y no tecnológicas
- Desarrollar:
 - Políticas de seguridad,
 - Estándares,
 - Procedimientos y normativas en general, que den forma a la cultura de seguridad informática
- La seguridad debe ser un facilitador de los negocios y no un obstáculo para realizarlos

Introducción

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



	MODELO DE NEGOCIO	
	TRADICIONAL	BASADO EN WEB
ENFOQUE	Seguridad estática Amenaza conocida	Seguridad Dinámica Amenaza Cambiante
FILOSOFIA	Usuarios desconocido se bloquea Acceso	Facilidad Acceso Seguros en el Mundo Virtual
FRECUENCIA DE AMENAZA	Esporádicas: Mensual o Menos	Constante
COSTO DE SEGURIDAD	Bajo o Moderado	Complejidad y Rapidez de Cambio Aumenta el Costo

Información: Atributos

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- Triada **CIA**: **C**onfidentiality, **I**ntegrity & **A**vailability
 - Preocuparse de la Seguridad de la Información significa, entre otros, proteger los activos de información, los sistemas de información y las redes que transportan dicha información, de cualquier daño resultante de posibles fallas en el cuidado de su Confidencialidad, Integridad o Disponibilidad (CIA).
 - Esta misión no está limitada sólo a las responsabilidades de un sistema informático y a su labor de procesar información, sino que está estrechamente ligada al éxito de la misión del negocio de la organización.

La Triada CIA

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



La Triada CIA

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



Confidencialidad

Una práctica efectiva para garantizar la confidencialidad de la información es implementar controles de acceso y autenticación, como contraseñas seguras y autenticación de dos factores.



Integridad

Para garantizar la integridad de la información, se pueden utilizar técnicas de cifrado y firmas digitales para asegurar que los datos no han sido modificados o manipulados sin autorización.



Disponibilidad

Para garantizar la disponibilidad de la información, es importante contar con un plan de continuidad del negocio que permita restaurar los sistemas y datos en caso de una interrupción o desastre.

Confidencialidad de la Información

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- **Confidencialidad**

- Asegura que la información es accesada únicamente por los usuarios autorizados.
- Requiere habilitar un nivel adecuado de control de la privacidad que permita proteger la información de una divulgación no autorizada.
- El tipo y nivel de control se establece en base a la clasificación de la información a proteger.

Confidencialidad de la Información

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- **Confidencialidad**

- Ej.: Existe información que posee un requerimiento mayor de protección de la Confidencialidad que otras, por ejemplo: Información Militar.
- Ej: monitoreo de red, “shoulder surfing”, acceso a archivos de passwords, ingeniería social.

Integridad de la Información

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- **Integridad**

- Mantenimiento de la completitud, exactitud y validez de la información, protegiéndola de modificaciones o alteraciones no autorizadas.
- Escenarios que evidencia problemas de Integridad:
 - Tipo 1: Usuarios no autorizados que pueden modificar la información.
 - Tipo 2: Usuarios autorizados que pueden efectuar modificaciones no autorizadas
 - Tipo 3: La información de los sistemas y su consistencia interna y con el exterior.

Integridad de la Información

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- **I**ntegridad

- Consistencia Interna: entre los registros de las bases de datos y entre valores parciales y totales.
- Consistencia Externa: entre los datos almacenados en los sistemas y los datos reales del mundo exterior.
- Ej.: Informes financieros tipo Memoria Anual de Sociedades Anónimas.
- Ej: Ataques a sistemas por virus, “logic bomb” o “back doors”.

Disponibilidad de la Información

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- **D**isponibilidad

- La información debe estar accesible en todo momento en que sea requerida.
- Para usuarios autorizados, no para cualquier usuario.
- De acuerdo a las condiciones establecidas en los acuerdos tipo SLA.

Disponibilidad de la Información

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- **Disponibilidad**

- Debe acordarse previamente las respuestas a:
 - ¿Cuándo?
 - ¿Dónde?
 - ¿Por cuánto?
 - ¿A quién?
- *Ej.: Acceso a información desde puntos de atención a usuarios POS.*
- *Ej: Ataques de DoS o DDoS*



Orígenes y Tipos de Atacantes

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



Orígenes y Tipos de Atacantes

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



Agenda ¿Quiénes son los atacantes?

Atacantes internos

Atacantes externos

Ataques de ingeniería social

Ataques de denegación de servicio

Conclusiones



¿Quiénes son los atacantes?

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



Un atacante es una persona o grupo

Busca aprovechar vulnerabilidades en sistemas informáticos para obtener información confidencial, dañar sistemas o interrumpir servicios.

Pueden ser internos o externos a la organización y utilizan diversas técnicas para lograr sus objetivos.

Es importante conocer a los atacantes y sus técnicas para poder protegerse de ellos.

Atacantes internos

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- Personas que trabajan dentro de la organización y tienen acceso a información confidencial.
- Estos individuos pueden dañar la organización de varias maneras:
 - Robando información
 - Causando daños a los sistemas.



Atacantes internos

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- Es importante identificar a estos atacantes y tomar medidas para prevenir sus acciones.
- Para prevenir ataques internos, es necesario
 - Establecer políticas claras de seguridad y monitorear el comportamiento de los empleados.
 - Implementar controles de acceso
 - Capacitaciones sobre seguridad de la información para concientizar a los empleados sobre los riesgos y las mejores prácticas



Atacantes externos

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- Son aquellos que intentan infiltrarse en la organización desde fuera.
- Entre ellos se encuentran
 - Hackers, crackers
 - phishers y otros delincuentes cibernéticos.
- Motivaciones.
 - Obtener información confidencial
 - Dañar la reputación de la organización
 - Causar caos.

Atacantes externos

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- Para lograr sus objetivos, los atacantes externos utilizan una variedad de técnicas de ataque, como el phishing, el malware y la ingeniería social.
 - El **phishing** es un método común en el que los atacantes envían correos electrónicos engañosos para obtener información confidencial, como contraseñas y números de tarjetas de crédito.
 - El **malware** es otro método popular en el que los atacantes infectan los sistemas con software malicioso para robar información o controlar los dispositivos.
 - La **ingeniería social** es una técnica en la que los atacantes manipulan a las personas para obtener información o acceso a los sistemas.



Ataques de ingeniería social

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



nacap

- Técnica utilizada por los atacantes para engañar a las personas y obtener información confidencial.
- Estos ataques suelen involucrar:
 - La manipulación psicológica o el engaño para que las víctimas revelen información personal o empresarial.
 - *Por ejemplo, un atacante podría hacerse pasar por un empleado de soporte técnico y pedirle a un usuario que revele su contraseña para solucionar un problema técnico.*



Ataques de ingeniería social

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



nacap

Aprovecha
sentimientos tan
variados como



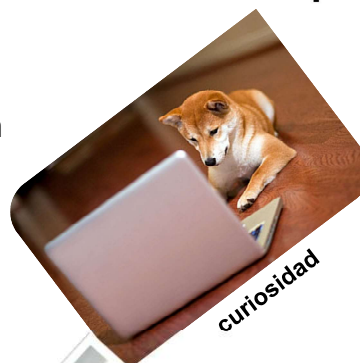
miedo



avaricia



compasión



curiosidad



sexo

Ataques de ingeniería social



- Para prevenir los ataques de ingeniería social:
 - Es importante educar a los empleados sobre cómo identificar y evitar estas técnicas de engaño.
- Algunas recomendaciones incluyen:
 - No compartir información confidencial por teléfono o correo electrónico.
 - Verificar la identidad de las personas antes de proporcionar información.
 - Tener políticas claras de seguridad de la información en la organización.

Clasificación de los atacantes

• Son personas con grandes conocimientos informáticos y telemáticos (expertos programadores).
• Por su infinita curiosidad dedican un gran esfuerzo a investigar los sistemas operativos y los sistemas de seguridad para descubrir todas sus vulnerabilidades.

Hackers:

• La palabra cracker proviene de Criminal HACKER, es decir hackers criminales, hackers cuyas intenciones son maliciosas

Crackers:

• Son expertos en telefonía. Son conocidos como los phone crackers, los crackers de la telefonía, buscan un beneficio económico saboteando las redes telefónicas para realizar llamadas gratuitas Phreakers

Phreakers:

• Son expertos en informática y en intrusismo en la red, que ponen sus conocimientos al servicio de países y organizaciones para el espionaje o sabotaje informático.

Ciberterroristas:

• Son expertos en programación, en sistemas y en redes, que crean pequeños programas dañinos, que por uno u otro motivo llegan a la red y se distribuyen con rapidez ocasionando daños en los sistemas o en la información almacenada en los mismos.

Programadores de virus:

• También conocidos como wannabes o script-kiddies o click-kiddies, son chicos jóvenes que, sin grandes conocimientos informáticos, se creen verdaderos hackers y se lo hacen creer a los miembros de sus pandillas.

Lammers:

• Son los hackers novatos, empiezan a aprender y van superando los primeros retos para llegar a ser verdaderos hackers.

Lammers Newbie:

Clasificación de los atacantes

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- Es un malware que tiene la propiedad de duplicarse a sí mismo.
- Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.
- Ejemplo:
 - I love you 2000 - >10.000.000.-
 - Código Rojo 2001 - 359.000 sistemas en menos de 14 horas.

Gusano:

- Simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco...), produciendo una negación de servicio.

Bacteria/Conejo:

- Programas que permanecen sin realizar ninguna función hasta que son activados; en ese punto, la función que realizan no es la Original del programa, sino que generalmente se trata de una acción Perjudicial.

Bomba lógica:

- Es un software que recopila información y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del computador.

Spyware:

- Programa que automáticamente muestra u ofrece publicidad no deseada, ya sea incrustada en una página web mediante gráficos, carteles, ventanas flotantes, o durante la instalación de algún programa al usuario, con el fin de generar lucro a sus autores.
- La palabra adware corresponde al conjunto de palabras "advertising" (publicidad) y "software" (programa), para referirse a sistemas de publicidad basados en programación computacional.

Adware:

Clasificación de los atacantes

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- Es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers que consiguen acceder ilícitamente a un sistema informático.

Rootkit:

- Un keylogger es un software o hardware que puede interceptar y guardar las pulsaciones realizadas en el teclado de un equipo que haya sido infectado.
- Este malware se sitúa entre el teclado y el sistema operativo para interceptar y registrar la información sin que el usuario lo note.

Keylogger:

- Atacan los sistemas de tarjetas, especialmente los cajeros automáticos.

Carders:

- Lo podríamos traducir como colilla, son las personas que se dedican a escuchar el tráfico de la red, para intentar recomponer y descifrar los mensajes que circulan por la misma.

Sniffers:

Ataques de denegación de servicio

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- Los ataques de denegación de servicio (DoS)
 - Son una forma de ataque cibernético que tiene como objetivo abrumar un sitio web o servidor con tráfico falso e inútil, lo que puede llevar a la caída del sistema.
 - Pueden ser realizados por individuos malintencionados o incluso organizaciones enteras con el objetivo de interrumpir el funcionamiento normal de un sitio web o servicio en línea.

Ataques de denegación de servicio

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- Para prevenir los ataques de denegación de servicio, es importante tener medidas de seguridad adecuadas en su lugar, como:
 - Firewalls y sistemas de detección de intrusos.
 - Monitorear regularmente el tráfico del sitio web y estar preparado para responder rápidamente si se detecta un ataque en curso.
- Si un sitio web o servicio en línea se ve afectado por un ataque de denegación de servicio, es importante tomar medidas para mitigar los efectos, como limitar el ancho de banda disponible para el atacante o bloquear el tráfico malicioso.

Ataques de Sistemas

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



De esta forma se consigue el objetivo, una acción por parte del usuario.



Conclusión

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- Conocer a los diferentes tipos de atacantes y sus técnicas es fundamental para proteger la organización.
 - Los atacantes internos pueden ser prevenidos mediante políticas de seguridad y monitoreo constante, mientras que los ataques externos requieren medidas adicionales como firewalls y sistemas de detección de intrusos.
 - Es importante educar a los usuarios sobre los riesgos de la ingeniería social y cómo prevenirla.
 - Finalmente, los ataques de denegación de servicio pueden mitigarse mediante la implementación de planes de contingencia y redundancia de servicios.
- No se debe subestimar la amenaza de los atacantes, estar siempre alerta y preparados para enfrentarlos.
- La seguridad no es una tarea fácil ni estática, sino un proceso continuo que debe ser actualizado y mejorado constantemente.

Mecanismos de Seguridad Pasiva y Activa.



UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



Agenda

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



¿Qué son los Mecanismos de Seguridad Pasiva y Activa?

Mecanismos de Seguridad Pasiva

Tipos de Mecanismos de Seguridad Pasiva

Mecanismos de Seguridad Activa

Tipos de Mecanismos de Seguridad Activa

¿Qué son los Mecanismos de Seguridad Pasiva y Activa?

- Es el conjunto de mecanismos y procedimientos de protección de las tecnologías de la información y las comunicaciones, tales como redes, sistemas y equipos que albergan información. Dicha información debe ser protegida salvaguardando su integridad, confidencialidad y disponibilidad.



Mecanismos de Seguridad Pasiva

La ciberseguridad pasiva (o seguridad reactiva) está formada por todos aquellos elementos que minimizan los efectos de un ciberataque una vez que se ha producido.

Se trata de poner en marcha todos los mecanismos necesarios para bloquear el ataque y recuperar la normalidad en el menor plazo de tiempo posible.

En esta fase es crucial contar con la ejecución de planes de respuesta ante ataques, planes de recuperación de información y elementos de análisis post mortem de los ataques.

Mecanismos de Seguridad Pasiva

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- Incluyen medidas que se ponen en marcha en el momento en que se produce un incidente de seguridad para minimizar los daños y recuperar la normalidad en el menor plazo de tiempo posible.

Mecanismos de Seguridad Pasiva

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



Escanear y desinfectar de malwares todos los equipos informáticos que se hayan visto afectados por esta intromisión en la seguridad.



Recuperar las copias de seguridad o backups más recientes con toda nuestra información guardada y en buen estado.



Realizar particiones de discos duros para almacenar las copias y evitar que el malware se extienda a más equipos.



Utilización de equipos adecuados para la protección contra accidentes y fallos de funcionamiento (refrigeración del sistema, conexiones eléctricas adecuadas, equipos SAI...).



Copias de seguridad de datos personales y de sistema operativo.

Mecanismos de seguridad activa

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- Corresponde a aquellos que tienen un carácter proactivo y su objetivo es prevenir que se produzcan incidentes de seguridad, tales como
 - Infecciones por malware.
 - Ataques de denegación de servicio
 - Robo de información, etc.

Tipos de Mecanismos de Seguridad Activa

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



Gestionar permisos de usuarios:

Definición e implantación de una política de gestión de los privilegios administrativos (permisos de administrador) de los usuarios de los sistemas. La utilización de estos usuarios posibilita y amplifica la ocurrencia de incidentes de seguridad ya que, por ejemplo, muchos tipos de malware necesitan de autorización para poder ejecutarse.



Gestionar credenciales de los usuarios:

Definición e implantación de una política robusta de contraseñas (complejidad, caducidad, etc.) que evite que estas puedan ser comprometidas (ataques de fuerza bruta, de diccionario...).



Controles antimalware:

Implantación de software antivirus en los equipos y sistemas de la organización.



Actualización y parcheo de seguridad de los sistemas y equipos:

Si presentan vulnerabilidades que no han sido corregidas mediante actualizaciones y parcheo, estas pueden ser explotadas por potenciales atacantes.



Backups:

Realización de copias de seguridad de la información de la organización y la configuración de los equipos y sistemas que permitan una rápida recuperación de la información en caso de pérdida de esta.

Tipos de Mecanismos de Seguridad Activa

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



Formación y concienciación en SIG del personal de las organizaciones:

- Las personas siempre son el eslabón más débil cuando hablamos de ciberseguridad.

Gestión de soportes extraíbles de información:

- Limitar el uso de este tipo de soportes o los permisos de escritura en los mismos para evitar posibles infecciones por malware o filtraciones de información.

Controlar el acceso a la red de dispositivos no controlados:

- Evitar que se conecten a la red dispositivos que puedan estar comprometidos.

Otras medidas:

- Gestión de dispositivos móviles (teléfonos, portátiles, tablets...). implantación de plataformas de seguridad perimetral (firewall, IPS/IDS...), etc.
- Implantación de plataformas de seguridad perimetral (firewall, IPS/IDS...), etc.

Normativas
ISO 27000,
ISO 27001,
ISO 27002:



UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA

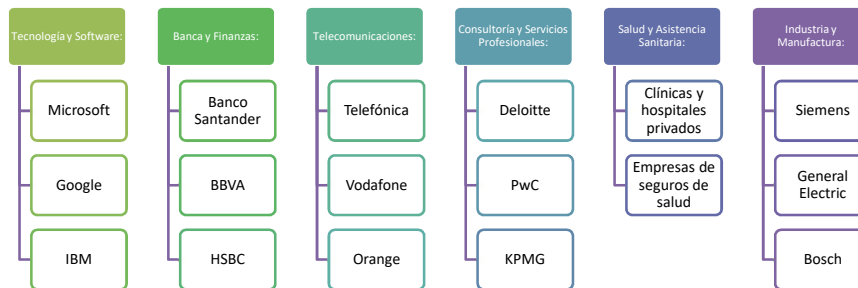


Normativa. ISO 27000. ISO 27001. ISO 27002.

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



Muchas empresas de diversos sectores buscan la certificación ISO 27001 para demostrar su compromiso con la seguridad de la información



Estas empresas buscan la certificación ISO 27001 para asegurar a sus clientes y socios que manejan la información de manera segura y conforme a las mejores prácticas internacionales¹.

Introducción

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- La ISO/IEC 27001 es un estándar internacionalmente reconocido que establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).
- Este estándar es parte de la familia ISO 27000, que aborda diversos aspectos de la gestión de la seguridad de la información.

Agenda

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



Introducción a la familia ISO 27000.

Detalle de la ISO 27001: Sistema de Gestión de la Seguridad de la Información.

ISO 27002: Controles de Seguridad de la Información.

Beneficios y desafíos de la implementación.

Conclusión.

Familia de Normas ISO 27000

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- Definición: Conjunto de normas que proveen un marco para la gestión de la seguridad de la información.
- ISO 27000: Visión general y vocabulario.
 - Proporciona un marco común de referencia para todas las normas de la serie.
- Introducción a los términos clave como SGSI (Sistema de Gestión de Seguridad de la Información).
- Interrelación de las Normas:
- ISO 27001: Requisitos para un SGSI.
- ISO 27002: Código de prácticas para la gestión de la seguridad de la información.
- Otras normas relacionadas (ISO 27005, ISO 27017, etc.).

Objetivo del Estándar ISO 27001

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- El principal objetivo de la ISO 27001 es garantizar que una organización adopte medidas adecuadas para proteger la confidencialidad, integridad y disponibilidad de la información, en función de los riesgos a los que esté expuesta.
- Establece la necesidad de gestionar adecuadamente los activos de información, asegurando que los recursos sean protegidos contra amenazas y vulnerabilidades.

ISO 27001:

Sistema de Gestión de Seguridad de la Información (SGSI)

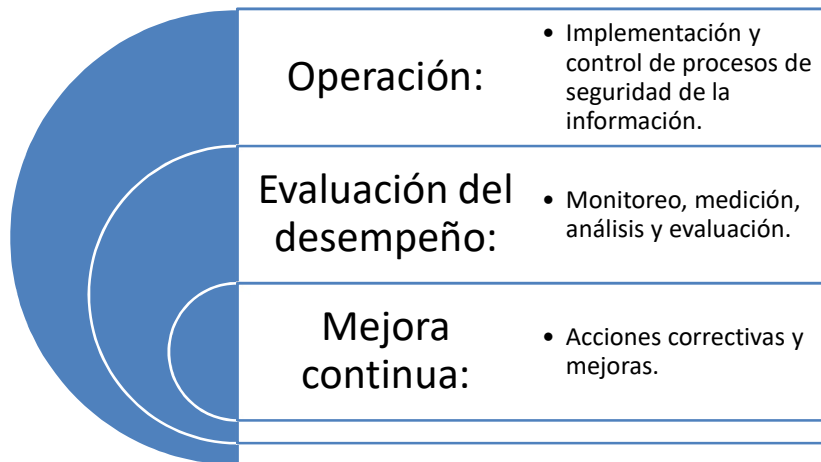
UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- Propósito: Establecer, implementar, mantener y mejorar continuamente un SGSI.
- Requisitos Clave:

ISO 27001: Sistema de Gestión de Seguridad de la Información (SGSI)

- Propósito: Establecer, implementar, mantener y mejorar continuamente un SGSI.
- Requisitos Clave:



ISO 27002: Controles de Seguridad de la Información



ISO 27001: Sistema de Gestión de Seguridad de la Información (SGSI)

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



Propósito General:

ISO 27001 es la norma internacional que describe cómo gestionar la seguridad de la información. Su propósito principal es proteger la confidencialidad, integridad y disponibilidad de la información en una organización mediante un proceso de gestión de riesgos.



Alcance:

Es aplicable a cualquier organización, sin importar su tamaño, sector o ubicación geográfica.

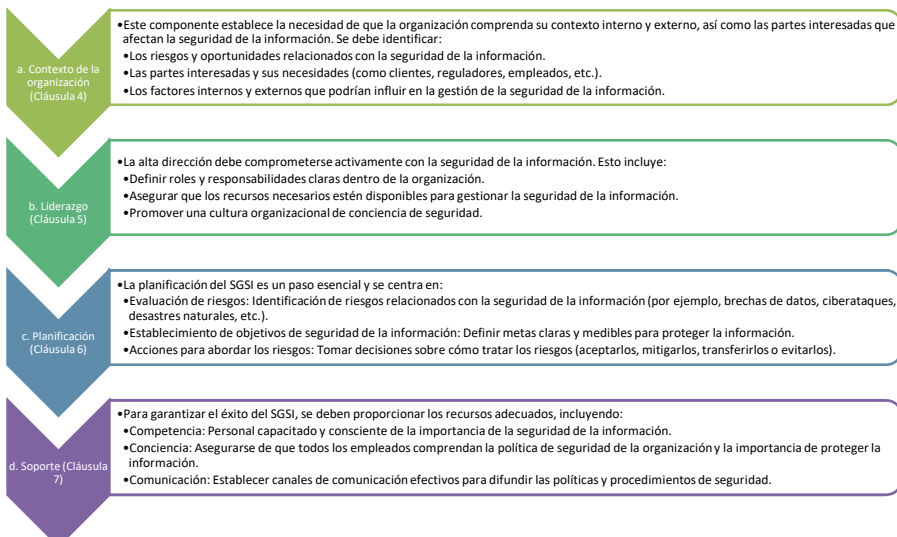


Estructura de la Norma ISO 27001

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA

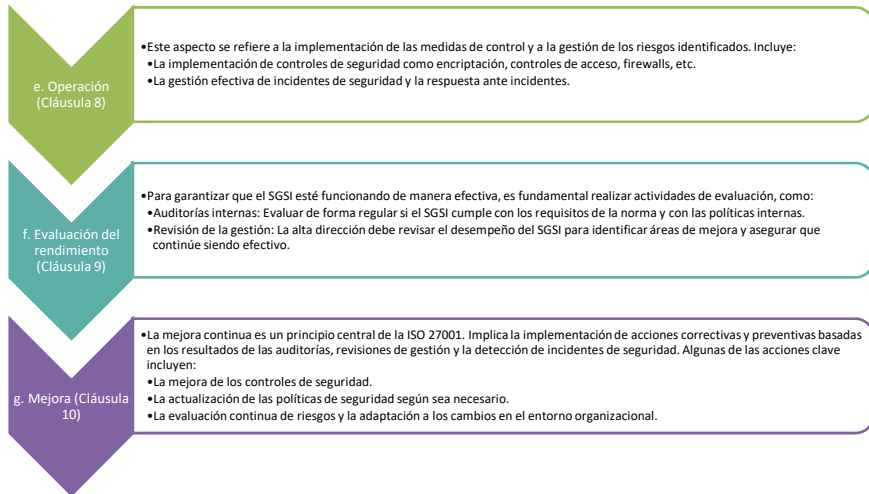


- La norma ISO 27001 se basa en un enfoque de gestión de riesgos e implementa los siguientes componentes clave:



Estructura de la Norma ISO 27001

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



Estructura de la Norma ISO 27001

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



Controles de Seguridad

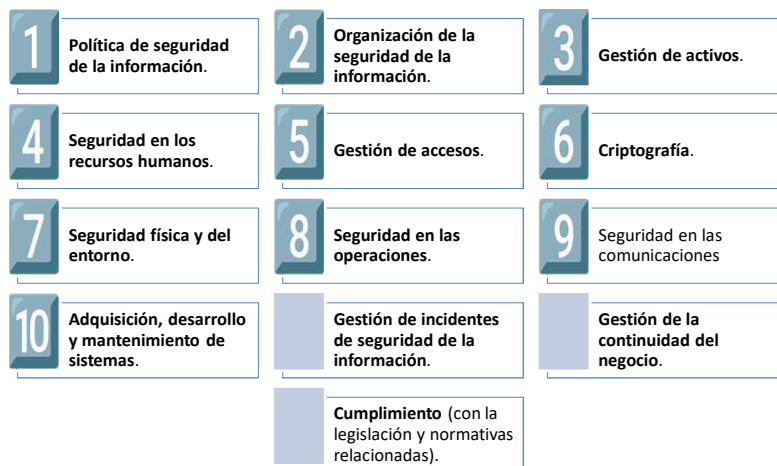
UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- El estándar ISO 27001:2013 incluye un conjunto de controles de seguridad descritos en el Anexo A.
- Estos controles se dividen en 114 controles de seguridad organizados en 14 dominios.
- Están diseñados para abordar aspectos específicos de la seguridad de la información, y las organizaciones deben seleccionar e implementar aquellos controles que sean relevantes para sus necesidades y riesgos.

Controles de Seguridad

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



Estos controles permiten a las organizaciones adaptar sus medidas de seguridad a sus necesidades específicas.

ISO 27001:2022

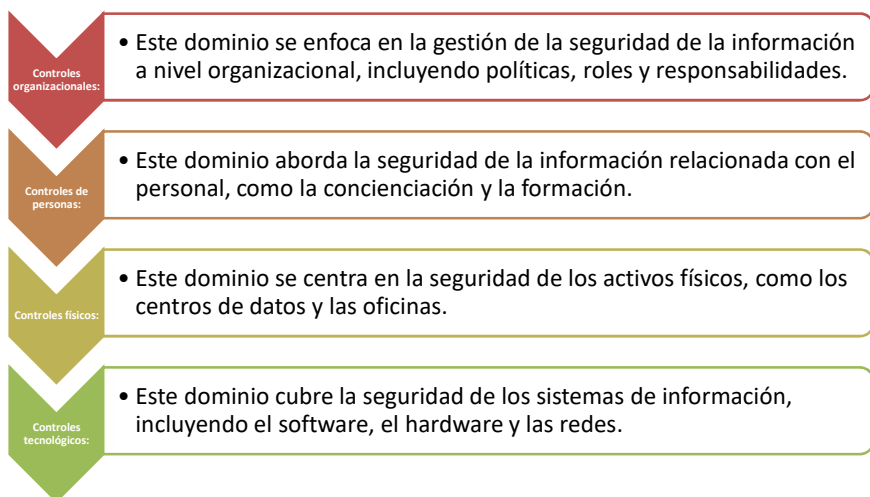
UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- La norma ISO 27001:2022 se centra en la gestión de la seguridad de la información y presenta algunos cambios en comparación con versiones anteriores.
- La estructura se divide en dos partes principales:
 - Cláusulas obligatorias: Incluyen 10 apartados que cubren temas como el contexto de la organización, liderazgo, planificación, apoyo, operación, evaluación de desempeño y mejora continua.
 - Anexo A: Contiene los controles específicos de seguridad, que ahora se han reducido y reorganizado en 93 controles distribuidos en 4 temas principales:
 - Controles organizativos.
 - Controles relacionados con las personas.
 - Controles tecnológicos.
 - Controles físicos.

Dominios ISO 27001:2022

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA

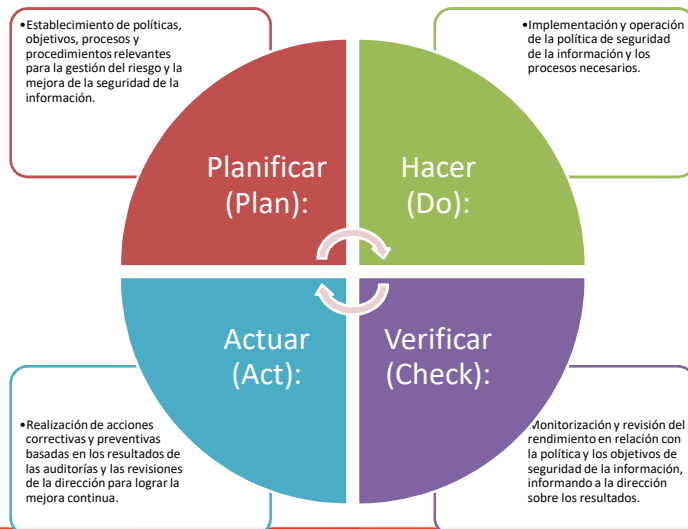


Estructura de la Norma ISO 27001

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



• 3.3. Ciclo PHVA (Planificar-Hacer-Verificar-Actuar)



Evaluación y Gestión de Riesgos

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



Evaluación de Riesgos:

Identificación de los activos de información.
Determinación de las amenazas y vulnerabilidades asociadas.
Evaluación de los impactos y probabilidades de que ocurran incidentes de seguridad.



Gestión de Riesgos:

Aceptación de riesgos:
• Decidir no aplicar controles a ciertos riesgos debido a su baja probabilidad o impacto.
Tratamiento de riesgos:
• Implementar controles para mitigar riesgos.
Transferencia de riesgos:
• Utilizar seguros u otros métodos para transferir el riesgo a terceros.
Evitar riesgos:
• Cambiar procesos para eliminar riesgos por completo

Estructura de la Norma ISO 27001

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



3.5. Declaración de Aplicabilidad (SoA)

Descripción:

- Documento clave que justifica por qué se seleccionan o no ciertos controles de seguridad. Debe alinearse con los resultados de la evaluación de riesgos y la política de seguridad de la información.

Propósito:

- Asegurar que todos los controles seleccionados sean implementados y que haya justificación para los controles no seleccionados.



Auditorías Internas:

Propósito:

- Verificar que el SGSI cumple con los requisitos de la norma y que se implementa y mantiene de manera efectiva.

Frecuencia:

- Deberían realizarse periódicamente, en función de la criticidad de los procesos.



Revisión por la Dirección:

Objetivo:

- Evaluar la adecuación, pertinencia y eficacia del SGSI.

Elementos:

- Resultados de auditorías, resultados de mediciones, incidentes de seguridad, retroalimentación de partes interesadas, etc.

Resultados:

- Decisiones sobre oportunidades de mejora, necesidades de cambios en el SGSI, y recursos necesarios.

Estructura de la Norma ISO 27001

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



• 3.7. Certificación ISO 27001



Estructura de la Norma ISO 27001

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



• 3.8. Beneficios de la Implementación de ISO 27001

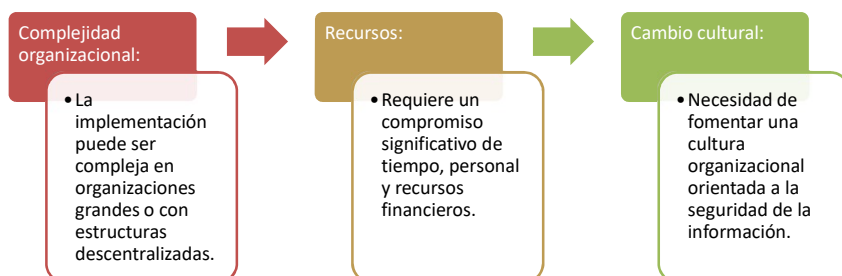


Estructura de la Norma ISO 27001

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



• 3.9. Desafíos en la Implementación



Preguntas

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA

