OTEC MSEREY
CENTRO DE ESTUDIO DE SEGURIDAD

PROTECCIÓN DE LA INFORMACIÓN Y CIBERSEGURIDAD

Curso Certified Protection Officer CPO IFPO

Marcelo Serey González
Ing. Prevención de Riesgos · CPO – CPOI – CSSM Asesor de Seguridad Privada

Agenda del Módulo

I. La información como activo

II. Marco legal y propiedad intelectual

III. Amenaza, vulnerabilidad y riesgo

IV. Espionaje y robo de alta tecnología

V. Mitigación y defensa en profundidad

VI. Programa de protección de la información

VII. Patrones de ataque y tipos de control

VIII. Ciberseguridad en Chile

IX. Sistema de Seguridad de la Información (SSI)

X. Fundamentos técnicos (AAA)

XI. Principios y propiedades de la seguridad

XII. Respuesta, recuperación y cierre

PARTE I

La Información como Activo

PARTE I · ACTIVOS DE INFORMACIÓN

¿Qué son los Activos de Información?

- Se componen de información confidencial, datos privados, propiedad intelectual y activos intangibles definidos por leyes de secretos comerciales, patentes y derechos de autor.
- Incluyen conocimiento científico, marca, reputación y procesos de negocio.
- **Formas en que existen los activos de información:**
- El conocimiento de una persona · la información oral · un proceso o procedimiento
- Información escrita en papel · datos en sistemas IT o de comunicaciones
- Una transmisión electrónica · datos almacenados en soportes (CD, USB, memoria, disco)

Ejemplos de Información Crítica

- Se denominan activos porque la información propietaria puede alterar dramáticamente el curso de la compañía, de forma positiva o negativa.
- Planes estratégicos, diseños, planos y propuestas
- Registros de investigación y desarrollo (I+D)
- Estrategias legales, acuerdos y contratos
- Contactos, listados de clientes e información personal de clientes
- Presupuestos, proyecciones y planes de adquisición y expansión
- Información personal relacionada con empleados

PARTE I · ACTIVOS DE INFORMACIÓN

Vivimos en el Mundo de los Datos

- El volumen y el valor de la información que generan y manejan las organizaciones crece de forma continua, y con él, su exposición a pérdida, robo o divulgación.
- Cada dato generado —oral, escrito, electrónico— es un activo que debe protegerse con el mismo cuidado que cualquier otro bien de la compañía.
- **La protección de la información ya no es una función aislada de TI: es una responsabilidad transversal a toda la organización.**

Consideraciones en la Protección

- **Los empleados constituyen el punto más vulnerable en un programa de protección de información de propiedad.**
- La causa principal de pérdida de información es la divulgación involuntaria por parte de una persona autorizada a conocerla.
- Presentaciones de ventas
- Seminarios, reuniones y convenciones de asociaciones
- Discusiones con proveedores
- Declaraciones fuera del predio de la empresa
- Declaraciones a la prensa, publicaciones y relaciones públicas

PARTE II

Marco Legal y Propiedad Intelectual

Información Propietaria vs. Confidencial

- **Información propietaria: posee elementos únicos, desarrollados por la empresa, que le otorgan una ventaja competitiva sobre otros.**
- Está protegida por ley bajo las categorías de secreto comercial, patente, marca registrada o derecho de autor.
- **Información confidencial: aquella que la empresa considera privada, aunque no siempre cumpla los requisitos legales de un secreto comercial.**
- Ambas requieren controles de acceso, marcado y acuerdos de confidencialidad para mantener su protección legal.

PARTE II · MARCO LEGAL

Secreto Comercial: Definición y Requisitos

- Fórmula, patrón, compilación, programa, dispositivo, método, técnica o proceso que otorga a su titular una ventaja frente a quienes no lo conocen.
- **Requisito 1 — Valor económico: debe generar una ventaja competitiva real o potencial por no ser de conocimiento general.**
- **Requisito 2 — Esfuerzos razonables de protección: el titular debe adoptar medidas concretas para mantenerlo en secreto (acceso restringido, marcado, acuerdos de confidencialidad).**
- Si no se protege activamente, se pierde el derecho legal a reclamarlo como secreto comercial, aun si fue robado.

Categorías del Secreto Comercial

- Técnica: fórmulas, diseños, procesos de fabricación, algoritmos y especificaciones de producto.
- Comercial: listas de clientes, estrategias de marketing, planes de negocio y proveedores.
- Financiera: estructuras de costos, márgenes, proyecciones y modelos de precios.
- Negativa: resultados de pruebas fallidas o caminos descartados que ahorran tiempo y dinero a un competidor si los conoce.
- **Cualquiera de estas categorías puede perder su protección legal si la empresa no demuestra esfuerzos razonables para mantenerla en secreto.**

Patentes

- **Derecho exclusivo otorgado por el Estado para explotar comercialmente una invención nueva, con aplicación industrial y no evidente.**
- Patente de utilidad: protege procesos, máquinas, composiciones de materia o mejoras funcionales — duración típica de 20 años.
- Patente de diseño: protege la apariencia ornamental de un producto, no su función.
- Patente de planta: protege variedades vegetales nuevas reproducidas asexualmente.
- A diferencia del secreto comercial, la patente exige revelar públicamente la invención a cambio de su protección exclusiva por tiempo limitado.

PARTE II · MARCO LEGAL

Derechos de Autor

- **Protege la expresión original de una obra —literaria, artística, de software o audiovisual— desde el momento de su creación.**
- No protege la idea en sí misma, sino la forma concreta en que fue expresada.
- En Chile se rige por la Ley N.º 17.336 sobre Propiedad Intelectual.
- Otorga al autor derechos exclusivos de reproducción, distribución y modificación de su obra por un plazo determinado.
- El registro no es obligatorio para su protección, pero facilita la prueba de autoría en caso de disputa.

PARTE II · MARCO LEGAL

Marca Registrada

- **Signo distintivo —nombre, logo, frase o combinación de ellos— que identifica productos o servicios de una empresa y los distingue de la competencia.**
- Protege la reputación e imagen de marca construida por la empresa en el mercado.
- Su registro otorga uso exclusivo y es renovable indefinidamente, a diferencia de una patente.
- El uso no autorizado de una marca registrada (falsificación) constituye una infracción legal y puede generar pérdidas reputacionales y económicas significativas.

Acuerdos de Confidencialidad (NDA)

- **Contrato que obliga a una parte a no divulgar información designada como confidencial, bajo sanciones civiles o penales.**
- Se firman con empleados, proveedores, socios y contratistas que tendrán acceso a información sensible.
- Deben definir claramente qué se considera información confidencial, su vigencia y las excepciones (información ya pública, obtenida legítimamente por otra vía, etc.).
- Es la principal herramienta legal para demostrar 'esfuerzos razonables de protección' exigidos para sostener un secreto comercial ante un tribunal.

PARTE II · MARCO LEGAL

Normativa Chilena de Protección de la Información

- Ley N.º 17.336 — Propiedad Intelectual: protege obras literarias, artísticas y científicas, incluido el software.
- Ley N.º 19.628 — Protección de la Vida Privada: regula el tratamiento de datos de carácter personal.
- Ley N.º 19.799 — Documentos y Firma Electrónica: da validez legal a documentos y firmas electrónicas.
- Ley N.º 21.459 — Delitos Informáticos: sanciona el acceso ilícito, sabotaje y ataques a sistemas informáticos.
- **Ley N.º 21.663 — Marco de Ciberseguridad: crea la Agencia Nacional de Ciberseguridad (ANCI) y establece obligaciones para instituciones críticas.**

Métodos Legales de Protección: Checklist

- Identificar y clasificar formalmente qué información es secreto comercial, confidencial o de uso restringido.
- Marcar los documentos y archivos con la clasificación correspondiente ('Confidencial', 'Uso Interno', etc.).
- Firmar acuerdos de confidencialidad (NDA) con empleados, proveedores y socios antes de compartir información sensible.
- Registrar patentes, marcas y derechos de autor cuando corresponda, para obtener protección exclusiva reconocida por ley.
- **Auditar periódicamente el cumplimiento de estas medidas: sin evidencia de protección activa, se pierde el respaldo legal.**

PARTE III

Amenaza, Vulnerabilidad y Riesgo

¿Qué es una Amenaza?

- **Cualquier circunstancia o evento con el potencial de causar daño a un activo de información mediante acceso no autorizado, destrucción, divulgación o modificación.**
- Puede ser intencional (un actor que busca explotar la información) o accidental (un error humano o una falla técnica).
- Puede originarse dentro de la organización (interna) o fuera de ella (externa).
- El primer paso de cualquier programa de protección es identificar qué amenazas son razonablemente probables para los activos de la empresa.

Cuatro Fuentes de Amenaza

- **Empleados no capacitados: cometen errores por desconocimiento de las políticas y procedimientos de protección.**
- **Empleados descontentos: motivados por venganza, dinero o ambición, sustraen o dañan información deliberadamente.**
- **Espionaje corporativo: competidores u organizaciones que buscan activamente información propietaria mediante inteligencia competitiva o métodos ilegales.**
- **Ataques externos: hackers, crackers y ciberdelincuentes que explotan vulnerabilidades técnicas desde fuera de la organización.**

¿Qué es una Vulnerabilidad?

- **Debilidad o brecha en un sistema, proceso o control que puede ser explotada por una amenaza para causar daño.**
- A diferencia de la amenaza (el agente que ataca), la vulnerabilidad es la condición que hace posible el ataque.
- Puede ser física (una puerta sin cerradura), técnica (software sin actualizar) o humana (falta de capacitación).
- **Sin vulnerabilidad no hay riesgo: una amenaza sin una brecha que explotar no representa un peligro real para el activo.**

¿Qué es Riesgo? (ISO 31000)

- **Riesgo = probabilidad de que una amenaza explote una vulnerabilidad, multiplicada por el impacto que ese evento tendría sobre el activo.**
- La norma ISO 31000 define riesgo como el efecto de la incertidumbre sobre los objetivos de la organización.
- Gestionar el riesgo no significa eliminarlo por completo, sino llevarlo a un nivel aceptable mediante controles proporcionados al valor del activo.
- El proceso de gestión de riesgo incluye: identificar, analizar, evaluar y tratar (mitigar, transferir, aceptar o evitar).

¿Qué es un Control?

- **Medida implementada para reducir la probabilidad de que una amenaza explote una vulnerabilidad, o para disminuir el impacto si esto ocurre.**
- Controles preventivos: evitan que el incidente ocurra (cerraduras, permisos de acceso, capacitación).
- Controles detectivos: identifican un incidente en curso o ya ocurrido (cámaras, alarmas, auditorías).
- Controles correctivos: reducen el impacto y restauran la normalidad después de un incidente (respaldos, planes de recuperación).

Amenaza vs. Vulnerabilidad

- **Amenaza: el agente o evento externo que busca o puede causar daño (un atacante, un incendio, un empleado descontento).**
- **Vulnerabilidad: la debilidad interna que permite que ese daño ocurra (una puerta sin llave, un sistema sin parches).**
- Sin vulnerabilidad, la amenaza no puede materializarse; sin amenaza, la vulnerabilidad no representa un riesgo activo.
- La gestión efectiva de seguridad actúa sobre ambos frentes: reduce vulnerabilidades y anticipa amenazas.

Hurto de la Información

- **Sustracción no autorizada de información propietaria, con o sin el conocimiento de su propietario legítimo.**
- Puede ocurrir por copia (el original permanece, pero la exclusividad se pierde) o por sustracción física del soporte que la contiene.
- Los medios más comunes incluyen dispositivos de almacenamiento portátiles, correo electrónico, impresión no autorizada y fotografía de pantallas o documentos.
- El daño no siempre es evidente de inmediato: muchas veces se detecta solo cuando el competidor ya está utilizando la información.

Espionaje Industrial

- Inteligencia competitiva: recopilación legal de información pública sobre competidores (informes, patentes, prensa).
- **Espionaje industrial: cuando esa recopilación cruza a métodos ilegales — infiltración, soborno o hurto de información propietaria.**
- Escuchas furtivas (eavesdropping): intercepción no autorizada de conversaciones o comunicaciones electrónicas mediante dispositivos ocultos.
- Piratería informática: acceso no autorizado a sistemas para extraer información sin dejar rastro evidente.
- La combinación de estas técnicas es habitual en operaciones de espionaje corporativo sofisticado.

Amenazas V/S Vulnerabilidades

Agente de Amenaza	Puede explotar esta vulnerabilidad	Resultando en esta amenaza
Malware	Falta de software antivirus	Infección por virus
Hacker	Servicios que se ejecutan en el servidor	Acceso no autorizado a la información confidencial
Usuario	Parámetro mal configurado en el sistema operativo	Mal funcionamiento del sistema
Fuego	Falta de extintores	Daños en las instalaciones y equipos, y posible pérdida de vidas
Empleado	Falta de capacitación o de cumplimiento de las normas Falta de auditoría	Intercambio de información de misión crítica Alteración de las entradas y salidas de datos de aplicaciones
Contratista	Mecanismos de control de acceso laxos	Robo de secretos comerciales
Agresor	Aplicación mal escrita Falta de configuración rigurosa del Firewall	Realización de un desbordamiento de búfer Ataque de denegación de servicio
Intruso	Falta de guardias de seguridad	Romper ventanas y robar computadores y dispositivos

PARTE IV

Espionaje y Robo de Alta Tecnología

Robo de Alta Tecnología

- **Sustracción de equipos, componentes o dispositivos que contienen información sensible: laptops, discos duros, servidores y dispositivos móviles.**
- A menudo el objetivo real no es el equipo en sí, sino los datos que almacena.
- 'Endurecer el blanco' (target hardening): dificultar el acceso físico mediante cifrado de disco, bloqueo de puertos USB, cables de seguridad y control de inventario de equipos.
- La pérdida de un solo dispositivo sin cifrar puede equivaler a la pérdida de toda la base de datos de clientes o de I+D de la empresa.

Piratería de Software

- **Uso, copia, distribución o modificación de software sin la licencia o autorización correspondiente del titular de los derechos.**
- Incluye instalar un mismo software con licencia única en múltiples equipos, distribuir copias no autorizadas o desactivar mecanismos de protección.
- Expone a la organización a sanciones legales bajo la Ley N.º 17.336 de Propiedad Intelectual y a riesgos de seguridad, ya que el software pirata frecuentemente contiene malware.
- La gestión de activos de software (licencias, inventario y auditorías periódicas) es la principal medida de control.

Patrón de Ataque de una Amenaza

- **Reconocimiento: el atacante identifica el objetivo y recopila información pública sobre la organización y sus activos.**
- **Desarrollo del acceso: busca una vulnerabilidad explotable — humana, física o técnica.**
- **Explotación: ejecuta el ataque aprovechando la brecha identificada para acceder al activo.**
- **Consolidación y salida: obtiene, copia o extrae la información y borra evidencia de su intrusión.**
- Reconocer este patrón permite ubicar controles en cada etapa, no solo al final del proceso.

PARTE V

Mitigación y Defensa en Profundidad

PARTE V · MITIGACIÓN Y DEFENSA

Mitigación de Riesgos

- **Proceso de reducir la probabilidad o el impacto de un riesgo identificado a un nivel aceptable para la organización.**
- Evitar: eliminar la actividad o condición que genera el riesgo.
- Reducir: aplicar controles que disminuyan la probabilidad o el impacto del evento.
- Transferir: trasladar el riesgo a un tercero (seguros, contratos con proveedores).
- Aceptar: asumir el riesgo residual cuando el costo de mitigarlo supera el beneficio.

PARTE V · MITIGACIÓN Y DEFENSA

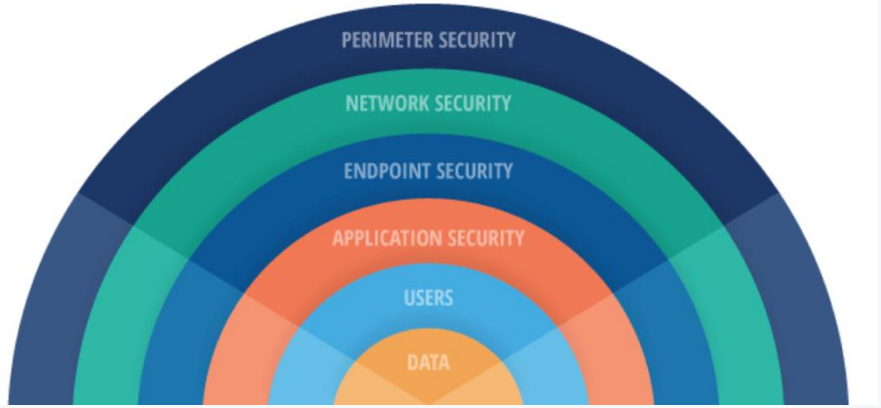
Elementos de Mitigación de Riesgos

- Políticas y procedimientos claros que definan cómo se clasifica, maneja y protege la información.
- Capacitación continua de los empleados sobre amenazas, vulnerabilidades y su rol en la protección.
- Controles técnicos (cifrado, autenticación, monitoreo) y físicos (acceso, cámaras, resguardo de equipos).
- Auditorías periódicas que verifiquen la efectividad real de los controles implementados.
- Un plan de respuesta a incidentes que permita actuar rápido cuando la prevención falla.

PARTE V · MITIGACIÓN Y DEFENSA

Defensa en Profundidad

- **Estrategia que combina múltiples capas de control independientes, de modo que si una falla, las siguientes siguen protegiendo el activo.**
- Capa de datos: cifrado, control de acceso a la información en sí, clasificación y respaldo.
- Capa de aplicación: control de vulnerabilidades del software, validación de entradas y gestión de parches.
- Capa de red: firewalls, segmentación, detección de intrusos y monitoreo del tráfico.
- Ningún control por sí solo es suficiente; la fortaleza está en la redundancia entre capas.



PARTE V · MITIGACIÓN Y DEFENSA

Capas Físicas y Administrativas

- Seguridad física: perímetro, control de acceso a instalaciones, vigilancia y protección de equipos críticos.
- Control de acceso: identificación, autenticación y autorización antes de permitir el ingreso a áreas o sistemas.
- Protección de datos: clasificación, cifrado y políticas de retención y eliminación segura.
- Supervisión: monitoreo continuo, auditorías y revisión de bitácoras de acceso.
- **Estas capas complementan las técnicas: sin control físico, incluso el mejor cifrado puede ser inútil si el equipo cae en manos equivocadas.**

Aplicaciones de la Defensa en Profundidad

- Un servidor con datos sensibles no depende solo del firewall: además exige autenticación, cifrado de disco, control de acceso físico al centro de datos y monitoreo de logs.
- Un empleado que maneja información propietaria está protegido por su NDA, su capacitación, los permisos de acceso limitados y la supervisión de su actividad.
- Un documento en papel se protege con clasificación, almacenamiento bajo llave, control de copias y protocolos de destrucción segura.
- **El principio es siempre el mismo: ninguna capa es infalible, pero juntas hacen mucho más costoso y difícil un ataque exitoso.**

Gestión de Seguridad: Necesidad de Conocer

- **Principio de 'necesidad de conocer' (need to know): el acceso a información sensible se otorga solo a quienes la requieren para cumplir su función, y nada más.**
- Reduce la superficie de exposición: menos personas con acceso significa menos puntos de fuga posibles.
- Se aplica combinando clasificación de la información con permisos de acceso diferenciados por rol.
- Debe revisarse periódicamente: los accesos otorgados por un proyecto puntual deben revocarse cuando éste finaliza.

PARTE VI

Programa de Protección de la Información

PARTE VI · PROGRAMA PIP

Política y Clasificación de la Información

- **Todo programa de protección de información (PIP) comienza con una política formal, aprobada por la dirección, que defina objetivos y alcance.**
- Clasificación por niveles: pública, interna, confidencial y secreta/restringida, cada una con reglas de manejo específicas.
- La política debe asignar responsables claros: quién clasifica, quién autoriza accesos y quién audita el cumplimiento.
- Sin una política escrita y comunicada, ningún control técnico o físico tiene respaldo institucional ni legal.

PARTE VI · PROGRAMA PIP

El Programa con los Empleados

- Inducción: todo nuevo empleado debe conocer la política de protección de información desde su primer día.
- Firma de acuerdos de confidencialidad como condición de acceso a información sensible.
- Capacitación periódica sobre amenazas actuales, phishing, ingeniería social y buenas prácticas de manejo de datos.
- Proceso de desvinculación: revocar accesos, recuperar equipos y recordar obligaciones de confidencialidad vigentes tras la salida.
- **El empleado informado y comprometido es el control más efectivo y menos costoso del programa.**

PARTE VI · PROGRAMA PIP

Otro Personal y Control de Acceso

- **Contratistas, proveedores y visitas representan un riesgo adicional: requieren su propio acuerdo de confidencialidad y acceso limitado al mínimo necesario.**
- Credenciales visibles y diferenciadas para identificar rápidamente a personal externo dentro de las instalaciones.
- Acompañamiento obligatorio de visitas en áreas restringidas.
- Registro de acceso: quién entra, a qué área, cuándo y con qué propósito — auditable en todo momento.
- Revisión de antecedentes antes de otorgar acceso a personal externo con funciones sensibles.

PARTE VI · PROGRAMA PIP

Medidas de Seguridad Física

- Perímetro: cercos, iluminación, control de accesos vehicular y peatonal en los límites de la propiedad.
- Edificio: cerraduras, tarjetas de acceso, torniquetes y recepción controlada en los puntos de entrada.
- Áreas críticas: salas de servidores, archivos y oficinas ejecutivas con control de acceso reforzado y biométrico si el riesgo lo justifica.
- Vigilancia: cámaras de circuito cerrado (CCTV), guardias y rondas periódicas que disuaden y documentan incidentes.

PARTE VI · PROGRAMA PIP

Protección de Documentos y de Información Electrónica

- **Documentación en papel: almacenamiento bajo llave, marcado de clasificación visible, control de copias y destrucción mediante trituración certificada.**
- **Información electrónica: cifrado en reposo y en tránsito, copias de respaldo periódicas y control de dispositivos de almacenamiento removibles.**
- Ambas formas requieren el mismo rigor: la protección de la información no depende del soporte, sino de su valor y sensibilidad.
- Todo documento o archivo debe tener un ciclo de vida definido: creación, uso, almacenamiento y disposición final segura.

PARTE VII

Patrones de Ataque y Tipos de Control

Patrón de Ataque Web

- **Escaneo: el atacante identifica sistemas expuestos, puertos abiertos y versiones de software vulnerables.**
- **Explotación: aprovecha una vulnerabilidad específica (inyección SQL, phishing, credenciales débiles) para obtener acceso.**
- **Escalamiento de privilegios: una vez dentro, busca ampliar su nivel de acceso hacia sistemas o datos más sensibles.**
- **Exfiltración y persistencia: extrae la información y, frecuentemente, deja puertas traseras para futuros accesos.**
- Cada etapa deja huellas que un monitoreo adecuado puede detectar antes de que el ataque se complete.

Tipos de Control

- Físicos: cerraduras, cercos, cámaras y guardias que restringen el acceso al entorno material.
- Técnicos (lógicos): cifrado, firewalls, autenticación y permisos que restringen el acceso a sistemas y datos.
- Administrativos: políticas, procedimientos, capacitación y auditorías que dirigen el comportamiento de las personas.
- **Un programa de protección robusto combina los tres tipos; ninguno sustituye completamente a los otros.**

Funcionalidad de los Controles

- **Preventivos: actúan antes del incidente, bloqueando el acceso no autorizado (cerraduras, permisos, cifrado).**
- **Detectivos: identifican que un incidente está ocurriendo o ya ocurrió (alarmas, cámaras, alertas de sistema).**
- **Correctivos: restauran la normalidad y reducen el daño después del incidente (respaldos, planes de continuidad).**
- **Disuasivos: desincentivan el intento de ataque sin necesariamente bloquearlo (avisos, iluminación, presencia visible de vigilancia).**
- Un control ideal combina varias de estas funciones a la vez.

PARTE VII · PATRONES Y CONTROLES

Controles Técnicos de Protección

- Cifrado de datos en reposo y en tránsito, para que la información sea inutilizable si es interceptada o sustraída.
- Autenticación multifactor (MFA) para reducir el riesgo de credenciales comprometidas.
- Firewalls y segmentación de red para contener el movimiento de un atacante dentro de la infraestructura.
- Sistemas de detección y respuesta (IDS/IPS, EDR) que identifican y contienen actividad anómala en tiempo real.
- Gestión de parches y actualizaciones para cerrar vulnerabilidades conocidas antes de que sean explotadas.

PARTE VIII

Ciberseguridad en Chile

Impacto de los Incidentes en Chile

- **Chile se encuentra entre los países de la región con mayor tasa de ciberataques por organización, según reportes de firmas como Check Point.**
- El sector público, financiero y de salud concentra los ataques de mayor impacto y visibilidad pública.
- Las pérdidas no son solo económicas: incluyen interrupción de servicios críticos, daño reputacional y pérdida de confianza de la ciudadanía.
- La creciente digitalización del país amplía la superficie de ataque, exigiendo marcos regulatorios y capacidades de respuesta más robustas.

PARTE VIII · CIBERSEGURIDAD EN CHILE

Marco Normativo Nacional

- **Ley N.º 21.459 — Delitos Informáticos: sanciona el acceso ilícito, sabotaje, interceptación y daño a sistemas informáticos, alineada con el Convenio de Budapest.**
- **Ley N.º 21.663 — Marco de Ciberseguridad e Infraestructura Crítica: establece obligaciones de reporte de incidentes y estándares mínimos de seguridad.**
- Crea la Agencia Nacional de Ciberseguridad (ANCI), organismo técnico encargado de coordinar la ciberseguridad a nivel nacional.
- Estas leyes obligan a instituciones públicas y operadores de infraestructura crítica a reportar incidentes dentro de plazos definidos.

PARTE VIII · CIBERSEGURIDAD EN CHILE

ANCI y CSIRT Nacional

- **Agencia Nacional de Ciberseguridad (ANCI): organismo técnico que coordina la política nacional de ciberseguridad y fiscaliza el cumplimiento normativo.**
- **CSIRT Nacional (Equipo de Respuesta a Incidentes de Seguridad Informática): coordina la respuesta técnica ante incidentes que afectan al Estado y a la infraestructura crítica.**
- Funciones principales: monitoreo de amenazas, alerta temprana, coordinación de respuesta y difusión de buenas prácticas.
- Las instituciones obligadas deben reportar incidentes significativos dentro de plazos establecidos por ley, bajo sanción de multas.

PARTE VIII · CIBERSEGURIDAD EN CHILE

Incidentes Reales en Chile

- SERNAC: sufrió un ciberataque que comprometió sistemas y expuso datos, afectando la atención a consumidores.
- Poder Judicial (CAPJ): un ransomware afectó sistemas informáticos, interrumpiendo tramitación de causas judiciales.
- Estado Mayor Conjunto (EMCO): filtración de información militar sensible tras un ciberataque de alto perfil.
- **Estos casos muestran que ninguna institución —pública o privada— está exenta, y que el impacto operacional puede ser tan grave como el económico.**

Modus Operandi de los Ataques

- **Ingeniería social: manipulación psicológica para que la víctima entregue información o realice una acción que compromete la seguridad.**
- **Phishing: correos o mensajes fraudulentos que simulan ser de una fuente confiable para robar credenciales o instalar malware.**
- **Malware: software malicioso diseñado para dañar, espiar o tomar control de un sistema sin autorización.**
- **Ransomware: cifra los archivos de la víctima y exige un pago (rescate) para restaurar el acceso.**
- Estos vectores suelen combinarse: un phishing exitoso es frecuentemente la puerta de entrada para instalar ransomware.

Tendencias de los Ataques

- Aumento sostenido del ransomware como servicio (RaaS), que permite a grupos con poca sofisticación técnica lanzar ataques complejos.
- Uso creciente de inteligencia artificial para automatizar y personalizar campañas de phishing.
- Ataques a la cadena de suministro: comprometer a un proveedor pequeño para alcanzar objetivos más grandes y mejor protegidos.
- Mayor foco en infraestructura crítica (energía, salud, servicios financieros) por su alto impacto social y de negociación.
- La tendencia general es hacia ataques más dirigidos, automatizados y difíciles de atribuir.

PARTE IX

Sistema de Seguridad de la Información (SSI)

PARTE IX · SISTEMA SSI

¿Qué es el SSI?

- **Sistema de Seguridad de la Información (SSI): conjunto integrado de políticas, procesos, personas y tecnologías orientado a proteger la confidencialidad, integridad y disponibilidad de la información.**
- No es un producto único, sino un marco de gestión continua que abarca toda la organización.
- Su objetivo es alinear la protección de la información con los objetivos estratégicos del negocio, no solo con requerimientos técnicos.
- Debe ser liderado por la alta dirección y sostenido con recursos, gobernanza y mejora continua.

Elementos del SSI

- Gobernanza: políticas, roles y responsabilidades definidas desde la alta dirección.
- Gestión de riesgos: identificación, análisis y tratamiento continuo de amenazas y vulnerabilidades.
- Controles: medidas físicas, técnicas y administrativas implementadas para proteger los activos.
- Personas: cultura de seguridad, capacitación y conciencia de todos los colaboradores.
- Monitoreo y mejora continua: auditorías, indicadores y ajuste permanente frente a nuevas amenazas.

Amenazas y Vulnerabilidades del SSI

- Amenazas típicas: fallas de energía, desastres naturales, fallas de hardware/software, errores humanos y ataques deliberados.
- Vulnerabilidades organizacionales: falta de políticas actualizadas, ausencia de capacitación y roles de seguridad mal definidos.
- Vulnerabilidades técnicas: sistemas sin parches, configuraciones por defecto y ausencia de monitoreo.
- **Un SSI eficaz identifica estas brechas de forma proactiva, antes de que se traduzcan en un incidente real.**

PARTE IX · SISTEMA SSI

Controles de Infraestructura

- Redundancia de energía (UPS, generadores) para asegurar continuidad ante cortes de suministro.
- Climatización y control ambiental en centros de datos para evitar fallas de hardware.
- Redundancia de conectividad y equipos críticos (servidores, switches) para evitar puntos únicos de falla.
- Respaldos periódicos y probados, almacenados en ubicaciones separadas del sitio principal.
- Planes de continuidad operativa y recuperación ante desastres (DRP) documentados y ensayados.

PARTE IX · SISTEMA SSI

Controles de Sistemas y de la Alta Dirección

- **Controles de sistemas de información: gestión de accesos, cifrado, monitoreo de logs y pruebas de vulnerabilidad periódicas.**
- **Controles de la alta dirección: aprobación de la política de seguridad, asignación de presupuesto y revisión periódica de indicadores de riesgo.**
- La dirección debe exigir reportes regulares sobre el estado del SSI y participar activamente en las decisiones de inversión en seguridad.
- **Sin patrocinio ejecutivo visible, los controles técnicos carecen de la autoridad y los recursos necesarios para sostenerse en el tiempo.**

PARTE X

Fundamentos Técnicos (AAA)

PARTE X · FUNDAMENTOS TÉCNICOS

Cómo Funcionan los Computadores y las Redes

- Un computador procesa información mediante hardware (procesador, memoria, almacenamiento) y software (sistema operativo y aplicaciones) que interactúan para ejecutar tareas.
- Una red conecta múltiples dispositivos para compartir información y recursos, mediante protocolos que definen cómo se transmiten los datos.
- Comprender esta arquitectura básica permite identificar en qué punto exacto se puede introducir una vulnerabilidad — dispositivo, sistema operativo, aplicación o canal de comunicación.
- La seguridad de la información depende de proteger cada uno de estos componentes de forma coordinada.

Términos Comunes de Infraestructura

- Servidor: equipo que provee servicios o recursos (archivos, correo, aplicaciones) a otros dispositivos de la red.
- Firewall: sistema que filtra el tráfico de red según reglas de seguridad definidas, bloqueando accesos no autorizados.
- VPN (red privada virtual): crea un canal cifrado para conexiones remotas seguras a la red corporativa.
- Nube (cloud): infraestructura y servicios alojados fuera de las instalaciones físicas de la organización, gestionados por un proveedor externo.
- Endpoint: cualquier dispositivo final conectado a la red (laptop, celular, impresora) y, por tanto, un punto potencial de entrada para un atacante.

Autenticación

- **Proceso de verificar que un usuario, dispositivo o sistema es efectivamente quien dice ser, antes de otorgarle acceso.**
- Factor de conocimiento: algo que el usuario sabe (contraseña, PIN).
- Factor de posesión: algo que el usuario tiene (token, tarjeta, celular con app de verificación).
- Factor de inherencia: algo que el usuario es (huella digital, reconocimiento facial).
- **La autenticación multifactor (MFA) combina al menos dos de estos factores, reduciendo drásticamente el riesgo de acceso no autorizado.**

PARTE X · FUNDAMENTOS TÉCNICOS

Identificación, Autenticación, Autorización y Trazabilidad

- **Identificación: el usuario declara quién es (nombre de usuario, credencial).**
- **Autenticación: el sistema verifica que esa identidad declarada es real (contraseña, biometría, token).**
- **Autorización: una vez verificada la identidad, el sistema determina a qué recursos puede acceder y qué acciones puede realizar.**
- **Trazabilidad (accountability): se registra cada acción del usuario autenticado, permitiendo reconstruir qué ocurrió, cuándo y quién lo hizo.**
- Estos cuatro elementos —conocidos como AAA (Authentication, Authorization, Accounting)— forman la base de todo control de acceso robusto.

PARTE XI

Principios y Propiedades de la Seguridad

PARTE XI · PRINCIPIOS Y PROPIEDADES

Principios Fundamentales de la Seguridad

- Menor privilegio: otorgar solo el acceso mínimo necesario para cumplir una función.
- Defensa en profundidad: múltiples capas de control, ya revisado en la Parte V.
- Separación de funciones: dividir tareas críticas entre varias personas para evitar abuso de poder individual.
- Falla segura: ante un error, el sistema debe negar el acceso por defecto, no otorgarlo.
- Simplicidad: los controles complejos son más difíciles de mantener y más propensos a errores de configuración.
- **Estos principios guían el diseño de cualquier control, sea físico, técnico o administrativo.**

PARTE XI · PRINCIPIOS Y PROPIEDADES

ISO 27001: Sistema de Gestión de Seguridad de la Información

- **Norma internacional que establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).**
- Se basa en el ciclo de mejora continua Planificar–Hacer–Verificar–Actuar (PHVA).
- Exige un análisis de riesgos formal y la selección de controles del Anexo A según los riesgos identificados.
- La certificación ISO 27001 es reconocida globalmente y demuestra a clientes y socios el compromiso de la organización con la protección de la información.

Riesgos en la Red

- Denegación de servicio (DoS/DDoS): saturación deliberada de un sistema para dejarlo inaccesible a usuarios legítimos.
- Inserción: introducción de código o datos maliciosos dentro de una comunicación o sistema en tránsito.
- Robo de información: intercepción de datos que circulan por la red sin cifrado adecuado.
- Modificación: alteración no autorizada de datos mientras viajan por la red, comprometiendo su integridad.
- Destrucción: eliminación deliberada de información o de la infraestructura que la soporta.

PARTE XI · PRINCIPIOS Y PROPIEDADES

Confidencialidad e Integridad

- **Confidencialidad: garantiza que la información solo sea accesible para las personas autorizadas a conocerla.**
- Se protege mediante cifrado, control de acceso, clasificación y acuerdos de confidencialidad.
- **Integridad: garantiza que la información sea exacta, completa y no haya sido alterada de forma no autorizada.**
- Se protege mediante control de versiones, funciones de verificación (hash), permisos de edición y registros de auditoría.
- Una filtración compromete la confidencialidad; una alteración no autorizada compromete la integridad — ambas son fallas distintas que requieren controles distintos.

PARTE XI · PRINCIPIOS Y PROPIEDADES

Disponibilidad y Autenticidad

- **Disponibilidad: garantiza que la información y los sistemas estén accesibles para los usuarios autorizados cuando los necesiten.**
- Se protege mediante redundancia, respaldos, planes de continuidad y protección frente a ataques de denegación de servicio.
- **Autenticidad: garantiza que la información y su origen son genuinos y no han sido falsificados o suplantados.**
- Se protege mediante firmas digitales, certificados y mecanismos de verificación de identidad del emisor.
- **Junto con confidencialidad e integridad, forman los cuatro pilares —CIDA— que sostienen cualquier estrategia de protección de la información.**

Seguridad Informática vs. Seguridad Física

- Seguridad informática: protege sistemas, redes y datos digitales mediante controles técnicos como cifrado, firewalls y autenticación.
- Seguridad física: protege instalaciones, equipos y personas mediante controles como cerraduras, vigilancia y control de acceso.
- Ambas convergen en sistemas integrados: por ejemplo, un sistema de vigilancia de video conectado a la red requiere protección tanto física (la cámara) como informática (los datos que transmite).
- **Un programa de protección de la información completo no separa estos dos dominios, sino que los coordina bajo una misma estrategia.**

PARTE XII

Respuesta, Recuperación y Cierre

PARTE XII · RESPUESTA Y CIERRE

Respuesta y Recuperación ante Incidentes

- Detección: identificar que un incidente está ocurriendo mediante monitoreo, alertas o reportes.
- Contención: aislar el sistema o área afectada para evitar que el daño se propague.
- Erradicación: eliminar la causa raíz del incidente (malware, acceso comprometido, vulnerabilidad explotada).
- Recuperación: restaurar sistemas y datos a su estado normal, usando respaldos verificados.
- Lecciones aprendidas: documentar el incidente y ajustar controles para evitar su repetición.

PARTE XII · RESPUESTA Y CIERRE

Destrucción Segura de la Información

- **Cuando la información deja de ser necesaria, debe eliminarse de forma segura para impedir su recuperación.**
- Documentos en papel: trituración certificada, no simplemente desecho en la basura común.
- Medios electrónicos: borrado seguro (wiping), desmagnetización o destrucción física del dispositivo de almacenamiento.
- Debe existir un registro de la destrucción: qué se destruyó, cuándo, cómo y quién lo autorizó.
- **La destrucción inadecuada es una de las formas más comunes —y evitables— de fuga de información.**

PARTE XII · RESPUESTA Y CIERRE

Impacto de un Incidente

- Impacto financiero: costos directos de remediación, multas regulatorias y pérdida de ingresos por interrupción operativa.
- Impacto reputacional: pérdida de confianza de clientes, socios e inversionistas, a menudo más duradera que el daño económico.
- Impacto legal: posibles demandas de clientes o socios afectados, y sanciones bajo la normativa de protección de datos y ciberseguridad.
- Impacto operacional: interrupción de procesos críticos que puede paralizar total o parcialmente la actividad de la organización.
- **El costo de prevenir un incidente es sistemáticamente menor que el costo de responder a uno ya ocurrido.**

PARTE XII · RESPUESTA Y CIERRE

Factores Críticos de Éxito

- **Compromiso visible de la alta dirección, con recursos y autoridad para sostener el programa en el tiempo.**
- **Cultura de seguridad compartida por todos los colaboradores, no solo por el equipo técnico.**
- **Controles proporcionados al valor real de los activos: ni sub-protección ni sobre-inversión innecesaria.**
- **Revisión y actualización continua frente a nuevas amenazas, tecnologías y cambios regulatorios.**
- Un programa exitoso no es el que nunca sufre un incidente, sino el que detecta, contiene y aprende rápido cuando ocurre.

OTEC MSEREY
CENTRO DE ESTUDIO DE SEGURIDAD

Proteger la información es proteger el negocio

Protección de la Información y Ciberseguridad