Fundamentos de Seguridad de Información
Unidad 2: Ética y legislación

Descargable

Índice

Introducción

En esta unidad, explorarás delitos informáticos y elementos normativos que se deben aplicar, de acuerdo con regulaciones nacionales e internacionales. Además, aprenderás temáticas relacionadas a Payment Card Industry Data Security Standard (PCI DSS) y a las responsabilidades legales relacionadas al crimen informático de acuerdo al convenio de Budapest. Por último, conocerás los aspectos fundamentales de La Ley 19.628 de Chile y su propuesta de actualización (Ley LPDP).

Elementos normativos nacionales e internacionales y delitos informáticos

Política Nacional de Ciberdefensa de Chile

Visión: Proteger la soberanía e intereses nacionales en el ciberespacio, asegurando un entorno seguro y resiliente.

Misión: Garantizar la defensa del ciberespacio chileno, protegiendo infraestructuras críticas y apoyando las operaciones de defensa en este ámbito.

Objetivos principales:

- **Protección del Ciberespacio:** Salvaguardar las infraestructuras críticas nacionales y los sistemas de información contra ciberataques y ciberespionaje.
- **Desarrollo de Capacidades:** Fortalecer las capacidades técnicas, humanas y organizacionales en ciberdefensa.
- **Resiliencia:** Aumentar la capacidad de respuesta y recuperación ante incidentes cibernéticos.
- **Colaboración y Coordinación:** Fomentar la cooperación interinstitucional y con el sector privado, así como la participación en alianzas internacionales.

Los siguientes son los fundamentos estratégicos de la Política Nacional de Ciberdefensa de Chile:

a) **Enfoque Integral**: Abordar la ciberdefensa de manera integral, considerando aspectos técnicos, organizacionales y normativos.

b) **Gestión de Riesgos**: Identificar y gestionar los riesgos cibernéticos de manera proactiva.

c) Actualización Continua: Adaptar continuamente la política y las estrategias a la evolución de las amenazas y las tecnologías.

d) **Soberanía Nacional:** Asegurar que las decisiones y acciones en ciberdefensa estén alineadas con la protección de la soberanía e independencia del país.

Los siguientes son los ejes estratégicos de la Política Nacional de Ciberdefensa de Chile:

- Fortalecimiento Institucional: Desarrollo y consolidación de capacidades institucionales dedicadas a la ciberdefensa, con roles y responsabilidades claramente definidos.
- Capacitación y Formación: Programas de educación y formación para el personal involucrado en ciberdefensa, así como para otros actores relevantes.
- Investigación y Desarrollo: Promoción de la investigación y el desarrollo en tecnologías y técnicas de ciberdefensa.
- Normativas y Regulaciones: Desarrollo de un marco normativo que respalde las operaciones de ciberdefensa y regule la protección de infraestructuras críticas.

Veamos algunos mecanismos de implementación:

- Coordinación Interinstitucional: Creación de comités y grupos de trabajo para la implementación y supervisión de la política.
- Inversiones en Tecnología: Adquisición e implementación de tecnologías avanzadas para la detección, protección y respuesta ante ciberataques.

- Simulacros y Ejercicios: Realización de simulacros regulares para evaluar y mejorar la preparación ante incidentes cibernéticos.

A continuación, revisemos dos aspectos de las relaciones internacionales:

- Cooperación internacional: Participación en redes y foros internacionales de ciberseguridad y ciberdefensa.
- Intercambio de Información: Colaboración en el intercambio de información sobre amenazas y mejores prácticas con otros países.

¿Cuáles son los principios de actuación de la Política?

- Proporcionalidad y Legitimidad: Las acciones de ciberdefensa deben ser proporcionales a la amenaza y respetar el marco legal.
- Transparencia: Mantener un grado de transparencia en las políticas y procedimientos de ciberdefensa, compatible con la seguridad nacional.
- Derechos Humanos: Respetar los derechos humanos y las libertades fundamentales en todas las actividades de ciberdefensa.

Marco Legal y Normativo

La política se articula dentro del marco legal existente y busca promover nuevas leyes y regulaciones que se adapten a la evolución del ciberespacio y sus amenazas.

Ley Marco sobre Ciberseguridad e Infraestructuras Críticas de la Información en Chile

La Ley 21.459 fue promulgada el 8 de diciembre de 2022. Esta ley establece un marco normativo integral para fortalecer la ciberseguridad en el país y proteger las infraestructuras críticas de la información (ICI).

Objetivo de la ley

- Protección de Infraestructuras Críticas de Información (ICI): Establece las bases para la identificación, protección y gestión de riesgos asociados a las ICI.
- Mejora de la Ciberseguridad Nacional: Proporciona un marco legal para mejorar la ciberseguridad en sectores estratégicos, promover la cooperación interinstitucional y asegurar la respuesta efectiva a incidentes cibernéticos.

Ámbito de Aplicación

- Sectores Críticos: La ley se aplica a sectores que proporcionan servicios esenciales cuya interrupción podría afectar la seguridad nacional, la economía o la salud pública.
- Organismos del Estado y Privados: Abarca tanto a entidades públicas como privadas que operan infraestructuras críticas.

Fundamentos principales de la Ley 21.459

La **Ley 21.459** se fundamenta en varios pilares esenciales:

a) Protección de ICI

- Identificación de ICI: Establece un proceso para identificar y catalogar las infraestructuras críticas de la información.
- Protección: Implementación de medidas técnicas y organizativas para proteger las ICI contra ciberamenazas.

b) Gestión de Riesgos

- Análisis de Riesgos: Obligación de realizar análisis de riesgos cibernéticos y establecer planes de gestión de estos riesgos.
- Controles de Seguridad: Implementación de controles adecuados para mitigar riesgos identificados.

c) Respuesta a Incidentes

- Planificación y Preparación: Desarrollo de planes de respuesta ante incidentes cibernéticos.
- Reportes de Incidentes: Obligación de reportar incidentes significativos a las autoridades competentes.

d) Coordinación y Cooperación

- Organismos de Coordinación: Creación de organismos y mecanismos de coordinación entre entidades públicas y privadas.
- Cooperación Internacional: Participación en redes y acuerdos internacionales para enfrentar ciberamenazas.

e) Capacitación y Concientización

- Formación Continua: Promoción de la formación en ciberseguridad para personal clave en la protección de ICI.
- Concientización: Campañas para sensibilizar sobre la importancia de la ciberseguridad en la sociedad.

Organismos y roles claves

La ley establece la creación y roles de diversos organismos para la implementación y supervisión de la ciberseguridad:

a) **Subsecretaría de Telecomunicaciones (Subtel):** Responsabilidades: Supervisar la implementación de medidas de ciberseguridad y coordinar la respuesta a incidentes cibernéticos en el sector de telecomunicaciones.

b) **Consejo Nacional de Ciberseguridad:** Sus funciones son asesorar al gobierno en políticas de ciberseguridad, promover la coordinación interinstitucional y formular estrategias nacionales.

c) **Centro Nacional de Ciberseguridad (CNC):** Su rol es operar como el centro de coordinación y respuesta ante incidentes cibernéticos, facilitando la comunicación y gestión de incidentes.

Medidas y obligaciones específicas

La ley define varias medidas y obligaciones para entidades responsables de ICI:

a) Planes de Ciberseguridad

Requisitos: Desarrollo e implementación de planes de ciberseguridad adaptados a la naturaleza de cada infraestructura crítica.

b) Controles de Seguridad

Medidas: Establecimiento de controles de seguridad, incluyendo protección contra malware, cifrado, y monitoreo de redes.

c) Auditorías y Evaluaciones

Frecuencia: Realización periódica de auditorías y evaluaciones de ciberseguridad para asegurar el cumplimiento y la efectividad de las medidas implementadas.

Principios orientadores

a) Proporcionalidad

Las medidas deben ser proporcionales al riesgo y la criticidad de la infraestructura.

b) Transparencia y Rendición de Cuentas

Las entidades deben ser transparentes en sus esfuerzos de ciberseguridad y rendir cuentas sobre su estado.

c) Resiliencia

Fomentar la resiliencia de las infraestructuras críticas ante ciberamenazas.

Sanciones y Cumplimiento

- **Infracciones:** La ley establece sanciones para entidades que no cumplan con las obligaciones establecidas.
- **Supervisión:** Autoridades competentes supervisan y evalúan el cumplimiento de la ley.

Ley de Delitos Informáticos de Chile

La Ley 19.223, también conocida como la Ley de Delitos Informáticos de Chile, fue promulgada el 7 de junio de 1993 y establece los delitos relacionados con la informática, así como sus sanciones. Esta ley es un pilar en la legislación chilena en materia de ciberseguridad y cibercrimen.

Objetivo de la Ley

El objetivo principal de la Ley 19.223 es tipificar y sancionar conductas delictivas en el ámbito informático, protegiendo la integridad y confidencialidad de los sistemas informáticos y los datos que contienen.

Ámbito de Aplicación

- **Delitos Informáticos:** La ley se aplica a delitos que involucran el uso de sistemas informáticos o datos, incluyendo la manipulación, acceso no autorizado y sabotaje de estos sistemas.
- **Sistemas Protegidos:** Incluye cualquier sistema de procesamiento de información, sea público o privado.

Fundamentos y delitos específicos

La Ley detalla varios delitos informáticos específicos y sus sanciones:

1. Acceso no Autorizado (Artículo 1)

- **Delito:** Acceder sin autorización a un sistema de tratamiento de información o mantenerse en dicho sistema.

- **Sanción:** Pena de presidio menor en su **grado mínimo (61 a 540 días)** o multa.

2. Sabotaje Informático (Artículo 2)

- **Delito:** Interrumpir o interferir el funcionamiento de un sistema de tratamiento de información, o destruir, dañar o alterar los datos.

- **Sanción:** Pena de presidio menor en su **grado medio (541 días a 3 años)** a **máximo (3 años y un día a 5 años).**

3. Manipulación de Datos (Artículo 3)

- **Delito:** Modificar, destruir, inutilizar o alterar datos almacenados en un sistema de tratamiento de información, sin autorización.

- **Sanción:** Pena de presidio menor en su **grado medio a máximo.**

4. Intercepción de Comunicaciones (Artículo 4)

- **Delito:** Interceptar, interferir o grabar comunicaciones no públicas transmitidas por medios informáticos.

- **Sanción:** Pena de presidio menor en su **grado medio a máximo.**

5. Difusión de Información (Artículo 5)

- **Delito:** Difundir o revelar información contenida en un sistema de tratamiento de información, obtenida sin autorización.

- **Sanción:** Pena de presidio menor en su **grado medio a máximo.**

6. Destrucción de Soportes (Artículo 6)

- **Delito:** Destruir, inutilizar o alterar soportes de almacenamiento o sistemas de tratamiento de información, afectando su funcionamiento.

- **Sanción:** Pena de presidio menor en su **grado medio a máximo.**

Fundamentos Legales y Conceptuales

- **Protección de la Información**

La ley reconoce la importancia de proteger la información y los sistemas de procesamiento contra accesos y manipulaciones no autorizadas.

- **Integridad de Sistemas**

Garantiza la integridad y disponibilidad de los sistemas de información, esenciales para el funcionamiento de entidades públicas y privadas.

- **Resguardo de la Confidencialidad**

Establece la necesidad de proteger la confidencialidad de la información, previniendo su acceso o divulgación no autorizada.

Las sanciones varían en función de la gravedad del delito, con penas que van desde presidio menor en sus diferentes grados hasta multas.

Actualizaciones y Relevancia

Aunque la Ley 19.223 fue pionera en su momento, la evolución de la tecnología ha planteado la necesidad de actualizar la normativa para abordar nuevos tipos de cibercrimen. En consecuencia, se han discutido y promulgado reformas y nuevas leyes para complementar y modernizar el marco legal en ciberseguridad y delitos informáticos en Chile.

Principios subyacentes

- **Legalidad:** Tipifica de manera precisa los comportamientos delictivos en el ámbito informático.
- **Proporcionalidad:** Establece sanciones que buscan ser proporcionales a la gravedad de la conducta delictiva.
- **Prevención:** Disuade conductas delictivas al establecer consecuencias claras para las mismas.
- **Protección de Derechos:** Busca proteger los derechos a la privacidad y a la propiedad sobre la información.

Normas internacionales: GDPR

Las **normas GDPR** (Reglamento General de Protección de Datos) e **HIPAA** (Ley de Portabilidad y Responsabilidad de Seguros Médicos) son **marcos regulatorios** que establecen estándares internacionales en la protección de datos personales y de salud. La Norma GDPR es un reglamento de la Unión Europea que entró en vigor desde el 25 de mayo de 2018.

Es uno de los **marcos legales más importantes** para la protección de datos personales. Su propósito es **garantizar la privacidad y protección** de datos personales dentro de la UE y regular la transferencia de datos personales fuera de la UE.

Fundamentos clave

Ámbito de Aplicación

- **Territorial:** Aplica a entidades que procesan datos de personas en la UE, independientemente de dónde estén ubicadas.
- **Material:** Cubre cualquier procesamiento de datos personales, con algunas excepciones (e.g., actividades personales o domésticas).

Principios del Tratamiento de Datos

- **Licitud, Lealtad y Transparencia:** Los datos deben ser procesados de manera lícita, leal y transparente.
- **Limitación de la Finalidad:** Los datos deben ser recogidos para fines específicos, explícitos y legítimos.
- **Minimización de Datos:** Los datos recolectados deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son procesados.
- **Exactitud:** Los datos deben ser exactos y, cuando sea necesario, actualizados.
- **Limitación de la Conservación:** Los datos deben mantenerse en una forma que permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento.
- **Integridad y Confidencialidad:** Los datos deben ser tratados de manera que se garantice una seguridad adecuada.

Derechos de los Interesados

- **Acceso:** Derecho a obtener confirmación sobre si se están tratando sus datos y a acceder a ellos.
- **Rectificación:** Derecho a corregir datos personales incorrectos.
- **Supresión:** Derecho a la eliminación de sus datos ("derecho al olvido").
- **Limitación del Tratamiento:** Derecho a limitar el procesamiento de sus datos.
- **Portabilidad de los Datos**: Derecho a recibir sus datos en un formato estructurado, de uso común y legible por máquina.
- **Oposición**: Derecho a oponerse al tratamiento de sus datos personales.
- **Decisiones Automatizadas:** Derecho a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado.

Obligaciones de los Responsables del Tratamiento

- **Consentimiento:** Obtención del consentimiento explícito e informado del interesado, salvo en ciertas excepciones.
- **Evaluaciones de Impacto:** Realización de evaluaciones de impacto sobre la protección de datos en caso de tratamientos que puedan implicar un alto riesgo para los derechos y libertades de las personas.
- **Medidas de Seguridad:** Implementación de medidas técnicas y organizativas apropiadas para garantizar la seguridad de los datos.
- **Notificación de Brechas:** Obligación de notificar a la autoridad de protección de datos y a los interesados en caso de violación de la seguridad de los datos

Transferencias Internacionales

- **Adecuación:** Transferencias a terceros países sólo si garantizan un nivel de protección adecuado.
- **Cláusulas Contractuales:** Utilización de cláusulas contractuales tipo o normas corporativas vinculantes para transferencias de datos internacionales.

Sanciones

Multas: Las sanciones por incumplimiento pueden llegar hasta el 4% de la facturación anual global de la empresa o 20 millones de euros, lo que sea mayor.

Supervisión

Autoridades de Protección de Datos: Cada Estado miembro de la UE debe contar con una autoridad de protección de datos que supervise el cumplimiento del GDPR.

Normas internacionales: HIPAA

La **HIPAA** (*Health Insurance Portability and Accountability Act*), promulgada en 1996 en Estados Unidos, se centra en la protección de la información de salud y establece normas para la seguridad y privacidad de los datos de salud, facilitando la portabilidad de los seguros de salud.

Fundamentos clave

Ámbito de Aplicación

Entidades Cubiertas: Se aplica a entidades cubiertas como proveedores de servicios de salud, planes de salud, y cámaras de compensación de atención médica.

Asociados Comerciales: También se aplica a los socios comerciales que manejan información protegida de salud (PHI) en nombre de entidades cubiertas.

Normas de Privacidad

- Protección de PHI: Garantizar la privacidad de la información protegida de salud, restringiendo su divulgación sin el consentimiento del individuo.
- Derechos del Paciente: Los pacientes tienen derecho a acceder y obtener una copia de su PHI, solicitar correcciones y obtener un informe de las divulgaciones de su PHI.
- Uso y Divulgación: La PHI puede ser usada y divulgada sin consentimiento para tratamiento, pago y operaciones de atención médica, con restricciones para otros fines.

Normas de Seguridad

- Confidencialidad, Integridad y Disponibilidad: Garantizar la confidencialidad, integridad y disponibilidad de la PHI electrónica.
- Protección contra Amenazas: Proteger contra amenazas razonablemente anticipadas para la seguridad o integridad de la PHI. Acceso Controlado: Asegurar que solo el personal autorizado acceda a la PHI.
- Evaluación de Riesgos: Realizar evaluaciones de riesgos periódicas para identificar y mitigar riesgos para la PHI.

Regla de Notificación de Brechas

Notificación Obligatoria: Requiere la notificación de las violaciones de PHI a las personas afectadas, a la Secretaría de Salud y Servicios Humanos (HHS), y en algunos casos, a los medios de comunicación.

Medidas de Seguridad Administrativas, Físicas y Técnicas

- Medidas Administrativas: Políticas y procedimientos para la gestión y protección de la PHI.
- Medidas Físicas: Controles para proteger los sistemas y equipos que manejan la PHI.
- Medidas Técnicas: Soluciones tecnológicas para proteger la PHI electrónica (ePHI), como cifrado y control de acceso.

Sanciones

Multas: HIPAA prevé sanciones por incumplimiento que pueden variar desde multas mínimas hasta millones de dólares por violaciones graves, incluyendo posibles sanciones penales.

Supervisión y Cumplimiento

HHS: La Oficina de Derechos Civiles del HHS es responsable de la supervisión y el cumplimiento de las normas HIPAA.

Payment Card Industry Data Security Standard

Payment Card Industry Data Security Standard es un conjunto de estándares de seguridad diseñado para proteger la información de las tarjetas de pago y reducir el riesgo de fraude. Es establecido por el Payment Card Industry Security Standards Council (PCI SSC),

Aplica a todas las entidades que almacenan, procesan o transmiten datos de tarjetas de crédito. Los fundamentos del PCI DSS se estructuran en torno a la protección de la información del titular de la tarjeta y la creación de un entorno seguro para las transacciones con tarjetas de pago.

Los fundamentos del PCI DSS se estructuran en torno a la protección de la información del titular de la tarjeta y la creación de un entorno seguro para las transacciones con tarjetas de pago.

Sus fundamentos cubren los siguientes aspectos: objetivo y alcance, ámbito de Aplicación, requisitos Principales, principios Orientadores, compliance y validación, y, por último, revisión y actualización de Estándares. Continúa el curso para saber más sobre estos fundamentos,

Fundamentos del PCI DSS

Propósito

- Protección de Datos de Tarjetas de Pago: Garantizar la protección de la información sensible del titular de la tarjeta contra el robo y el fraude.
- Establecimiento de Buenas Prácticas: Proveer un marco de estándares y buenas prácticas de seguridad para todas las organizaciones que manejan datos de tarjetas de pago.

Ámbito de aplicación

- Entidades: Abarca a todos los comerciantes, procesadores de pagos, instituciones financieras, y proveedores de servicios que manejan datos de tarjetas de crédito.
- Datos: Incluye datos del titular de la tarjeta, como el número de la tarjeta, la fecha de expiración, el código de seguridad (CVV), y cualquier otra información relacionada con la tarjeta.

Requisitos principales

El PCI DSS se compone de **12 requisitos fundamentales** que se agrupan en 6 objetivos de control. Cada requisito incluye diversos sub-requisitos y controles específicos.

1. **Construir y Mantener una Red Segura.** Instalar y Mantener una Configuración de Firewall para Proteger los Datos de los Tarjetahabientes:
    - Implementar firewalls para restringir el acceso no autorizado y proteger la red.
    - Establecer y mantener configuraciones seguras.

    No Utilizar Contraseñas y Otros Parámetros de Seguridad por Defecto de los Proveedores:
    - Cambiar contraseñas y configuraciones predeterminadas.
    - Asegurar que no se utilicen configuraciones predeterminadas en dispositivos de seguridad.

2. **Proteger los Datos del Titular de la Tarjeta.** Proteger los Datos Almacenados del Titular de la Tarjeta:

    Minimizar el almacenamiento de datos sensibles y proteger los datos que se retienen.

    Cifrar, truncar, y tokenizar datos sensibles.

    Cifrar la Transmisión de Datos del Titular de la Tarjeta a Través de Redes Abiertas y Públicas:

    Usar cifrado fuerte para proteger datos en tránsito.

Asegurar que la información de las tarjetas se transmita de manera segura.

3. **Investigación y Desarrollo.** Promoción de la investigación y el desarrollo en tecnologías y técnicas de ciberdefensa.
4. **Mantener un Programa de Gestión de Vulnerabilidades.** Usar y Mantener Programas de Protección Contra Malware y Asegurar que Se Actualicen Regularmente:
   - Implementar software anti-malware y actualizarlo regularmente.
   - Monitorear y proteger los sistemas contra malware.

   Desarrollar y Mantener Sistemas y Aplicaciones Seguras:
   - Establecer prácticas seguras de desarrollo de software.
   - Aplicar parches de seguridad oportunamente.
5. **Implementar Medidas Fuertes de Control de Acceso.** Restringir el Acceso a los Datos del Titular de la Tarjeta Según la Necesidad de Conocer la Información:
   - Limitar el acceso a datos sensibles a los empleados y sistemas con una necesidad legítima.
   - Aplicar principios de acceso mínimo y segregación de funciones.

Identificar y Autenticar el Acceso a Componentes del Sistema:

- Asignar identificadores únicos a cada persona con acceso a datos.
- Utilizar autenticación multifactor (MFA).

Restringir el Acceso Físico a los Datos del Titular de la Tarjeta:

- Proteger físicamente los datos almacenados.

- Implementar controles de acceso físico en instalaciones de datos.

6. Monitorear y Probar Regularmente las Redes

Rastrear y Monitorear Todos los Accesos a Recursos de la Red y Datos del Titular de la Tarjeta:

- Implementar registros de auditoría para todos los accesos y actividades.
- Monitorizar y revisar los registros regularmente.

Probar Regularmente los Sistemas y Procesos de Seguridad:

- Realizar pruebas de vulnerabilidad y escaneos periódicos.
- Implementar pruebas de penetración y evaluaciones de seguridad.

7. Mantener una Política de Seguridad de la Información

Mantener una Política que Aborde la Seguridad de la Información para Todo el Personal:

- Desarrollar, mantener y comunicar políticas de seguridad.
- Proveer formación y concienciación en seguridad a los empleados.

Principios orientadores

- Cifrado y Protección de Datos: Los datos del titular de la tarjeta deben cifrarse en tránsito y, cuando sea necesario, también en reposo para evitar el acceso no autorizado.
- Minimización de Datos: Solo almacenar la cantidad mínima de datos necesaria para el negocio y durante el menor tiempo posible.

- Segmentación de la Red: Segmentar la red para separar los sistemas de datos de tarjetas de otros sistemas, reduciendo así el alcance y el riesgo de comprometer los datos.

- Autenticación Fuerte: Utilizar métodos de autenticación robustos y asegurar que los accesos se gestionen de manera controlada y monitoreada.

Compliance y validación

- **Evaluaciones Anuales:** Realizar evaluaciones de cumplimiento anuales, que pueden incluir la revisión por un Auditor de Seguridad Calificado (QSA) o la realización de un autoevaluación.

- **Reportes de Cumplimiento:** Generar y presentar Reportes de Cumplimiento (ROC) y Atestaciones de Cumplimiento (AOC) según lo requiera la entidad adquirente o el banco.

- **Monitoreo Continuo:** Implementar medidas de monitoreo continuo para asegurar el cumplimiento continuo con el PCI DSS y responder rápidamente a cualquier incidente de seguridad.

Revisión y actualización de estándares

- **Versión Actualizada:** La norma PCI DSS se revisa y actualiza periódicamente para abordar nuevas amenazas y mejorar la seguridad. La versión más reciente a fecha de mi conocimiento es PCI DSS v4.0.

- **Participación de la Comunidad:** Las actualizaciones se realizan con la contribución de la comunidad global de pagos, incluidos comerciantes, bancos y proveedores de tecnología.

Convenio de Budapest

El Convenio de Budapest (también conocido como el Convenio sobre Ciberdelincuencia), firmado en 2001, es el **primer tratado internacional** destinado a abordar los delitos cometidos a través de Internet y otras redes informáticas.

Desarrollado por el Consejo de Europa con la participación de Estados Unidos, Canadá, Japón, y otros países, establece un marco legal común para la **lucha contra la ciberdelincuencia**.

- **Objetivos del convenio**
    - Combatir la Ciberdelincuencia: Proporcionar un marco común para **combatir el crimen** en el ciberespacio, incluyendo el acceso ilegal, la manipulación de datos y otros actos maliciosos.
    - Armonizar Legislaciones Nacionales: Facilitar la armonización de las legislaciones nacionales relacionadas con la ciberseguridad y la ciberdelincuencia.
    - Promover la Cooperación Internacional: Mejorar la **cooperación entre los países signatarios** para la prevención, investigación y persecución de delitos informáticos.

- **Fundamentos principales**

  El convenio se fundamenta en varios pilares esenciales:

  Tipificación de Delitos Informáticos

  El convenio define y establece la necesidad de tipificar varios delitos relacionados con la informática:

  - Acceso Ilegal: Acceso no autorizado a un sistema informático (Artículo 2).
  - Intercepción Ilegal: Intercepción no autorizada de datos (Artículo 3).
  - Interferencia de Datos: Daño o alteración de datos informáticos (Artículo 4).

- Interferencia de Sistemas: Interferencia con el funcionamiento de sistemas informáticos (Artículo 5).
- Abuso de Dispositivos: Posesión, producción, venta, adquisición, importación o distribución de dispositivos diseñados para cometer delitos informáticos (Artículo 6).

Delitos Relacionados con el Contenido

Tipifica actos relacionados con contenidos ilícitos:

- Pornografía Infantil: La producción, distribución, ofrecimiento y posesión de pornografía infantil (Artículo 9).

Delitos Relacionados con la Propiedad Intelectual

Incluye medidas para combatir infracciones relacionadas con los derechos de autor:

- Infracción de Derechos de Autor: Actos relacionados con la violación de derechos de propiedad intelectual en el entorno digital (Artículo 10).

Medidas procesales

Preservación de Datos

- Preservación de Datos Almacenados: Obliga a los Estados a establecer procedimientos para preservar datos informáticos esenciales para investigaciones (Artículo 16).
- Preservación Rápida de Tráfico de Datos: Preservación rápida de datos de tráfico en casos específicos (Artículo 17).

Acceso a Datos

- Orden de Aprehensión de Datos: Habilita la aprehensión de datos en posesión de una persona o entidad (Artículo 18).

- Acceso a Sistemas Informáticos: Proporciona a las autoridades la capacidad de acceder a sistemas informáticos para recopilar datos (Artículo 19).

Intercepción de Datos

Intercepción de Datos de Contenidos: Facilita la interceptación de datos en tiempo real, bajo ciertas condiciones (Artículo 21).

Cooperación Internacional

a. Cooperación Rápida

- Asistencia Técnica y Asesoría: Proporciona mecanismos para la asistencia mutua rápida y eficaz entre los países miembros (Artículo 25).
- Solicitud de Información: Facilita la solicitud y obtención de información y pruebas de otros países (Artículo 27).

b. Extradición

Extradición de Delincuentes: Establece reglas para la extradición de personas acusadas de delitos informáticos entre países miembros (Artículo 24).

Principios orientadores

Proporcionalidad y necesidad: Las medidas adoptadas en virtud del convenio deben ser proporcionales al delito y necesarias para su prevención y persecución.

Protección de Derechos Humanos

-Privacidad: Las medidas de ciberseguridad deben respetar la privacidad y otros derechos humanos (Artículo 15).

-Transparencia: Las acciones deben ser transparentes y acordes con los principios del estado de derecho.

Organización y Seguimiento

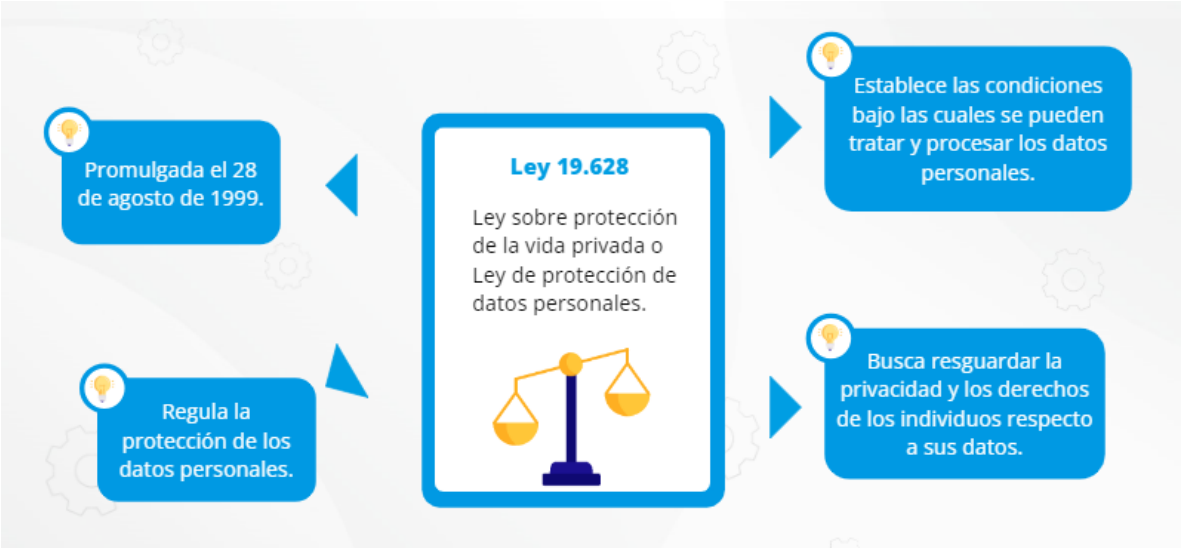
Comité del Convenio:
Supervisión y Evaluación: El comité supervisa la implementación del convenio y propone enmiendas para su actualización (Artículo 46).

Impacto global

- Modelo para Legislaciones Nacionales: El convenio ha servido como modelo para la legislación de muchos países, incluso de aquellos que no son miembros del Consejo de Europa.

- Adopción Internacional: Más de 60 países han firmado el convenio, reflejando su importancia global en la lucha contra la ciberdelincuencia.

Ley 19.628 (propuesta Ley LPDP)



Objetivo de la Ley

- **Protección de Datos Personales**: Garantizar la protección de los datos personales de las personas naturales frente a su tratamiento en bases de datos públicas y privadas.
- **Regulación del Tratamiento de Datos:** Establecer un marco legal para la recolección, almacenamiento, procesamiento y distribución de datos personales.

Ámbito de Aplicación

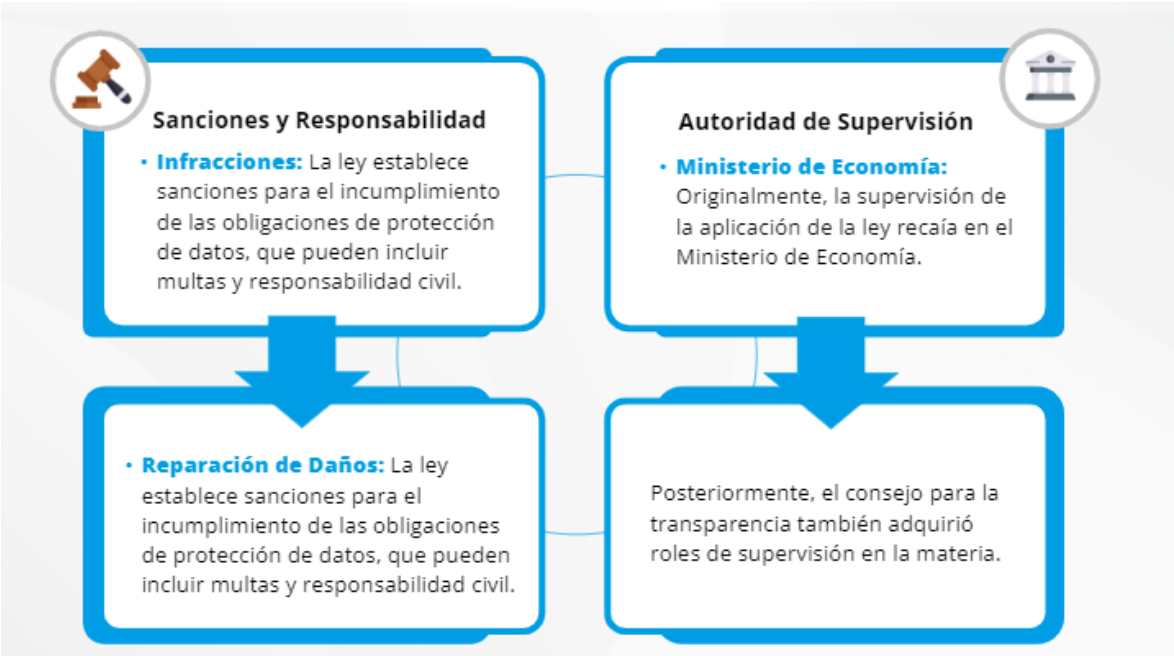
- **Datos Personales:** Se refiere a cualquier información concerniente a personas naturales, identificadas o identificables.
- **Responsables de Bases de Datos:** Aplica a personas y entidades, tanto del sector público como privado, que administran bases de datos personales.

Medidas de Seguridad

Obligación de Seguridad: Los responsables de bases de datos deben adoptar medidas técnicas y organizativas para garantizar la seguridad de los datos y evitar su alteración, pérdida, tratamiento o acceso no autorizado.

Transferencia de Datos

Regulación de Transferencias: La transferencia de datos personales a terceros, tanto dentro como fuera del país, debe garantizar un nivel adecuado de protección de los datos.



Fundamentos principales y principios subyacentes de la Ley

Principios de Tratamiento de Datos

- Licitud: El tratamiento de datos debe realizarse conforme a la ley y con respeto a los derechos y libertades de los individuos.
- Finalidad: Los datos deben ser recolectados con una finalidad específica, explícita y legítima.
- Proporcionalidad: El tratamiento de datos debe ser adecuado, pertinente y no excesivo en relación con la finalidad para la cual se recogen.
- Calidad de Datos: Los datos deben ser exactos, actualizados y completos en la medida de lo necesario para su tratamiento.
- Transparencia: Los individuos deben ser informados sobre el tratamiento de sus datos, incluyendo la finalidad y el responsable del tratamiento.

Consentimiento

Requisito del Consentimiento: El tratamiento de datos personales requiere el consentimiento previo, informado y expreso del titular de los datos, salvo en las excepciones legales establecidas.

Derechos de los Titulares

- **Acceso:** Derecho a saber qué datos personales suyos están siendo tratados.
- **Rectificación:** Derecho a solicitar la corrección de datos incorrectos o incompletos.
- **Cancelación:** Derecho a solicitar la eliminación de sus datos cuando ya no sean necesarios o se traten de manera incorrecta.
- **Oposición:** Derecho a oponerse al tratamiento de sus datos por razones legítimas

Principios subyacentes

- **Derecho a la Privacidad:** La ley se basa en el reconocimiento del derecho fundamental a la privacidad de las personas y la protección de su información personal.
- **Proporcionalidad y Minimización de Datos:** Se promueve el principio de proporcionalidad en el tratamiento de datos, limitando la recolección y uso de datos personales a lo estrictamente necesario para la finalidad prevista.
- **Transparencia y Confianza:** La ley busca fomentar la confianza en el manejo de datos personales mediante la transparencia en el tratamiento y la información proporcionada.

En síntesis, la Política Nacional de Ciberdefensa de Chile se enfoca en proteger el ciberespacio nacional mediante un enfoque integral que incluye la protección de infraestructuras críticas, el desarrollo de capacidades, la cooperación interinstitucional y la participación en foros internacionales, basado en principios de transparencia, proporcionalidad y respeto a los derechos humanos. La Ley 21.459 proporciona un marco normativo integral para fortalecer la ciberseguridad en Chile y proteger las infraestructuras críticas de información, mediante la identificación y protección de ICI, la gestión de riesgos, la mejora de la respuesta a incidentes, y la promoción de la cooperación interinstitucional e internacional, asegurando un entorno cibernético seguro y resiliente para el país.

Por otro lado, la Ley 19.223 establece el marco legal para sancionar delitos informáticos en Chile, protegiendo la integridad y seguridad de los sistemas y datos informáticos. Junto con otras normativas como el GDPR, HIPAA y PCI DSS, que establecen estándares de protección de datos personales, información de salud y datos de tarjetas de crédito, respectivamente, se complementan con el Convenio de Budapest, que promueve la cooperación internacional en la lucha contra la ciberdelincuencia, y la Ley 19.628, que garantiza el manejo seguro y respetuoso de la información personal, formando un entramado legal robusto que protege diversos aspectos de la seguridad y privacidad en el ámbito digital.

Bibliografia

- **Branden Williams, & Anton Chuvakin.** (2016). *PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance* (4th ed.). Syngress. doi:10.1016/B978-0-12-802048-0.00001-7
- **Contreras, R. (2020).** *Protección de datos personales en Chile: Avances y pendientes en el marco del proyecto de Ley LPDP*. Revista Chilena de Derecho, 27(1), 35-60.
- **European Parliament and Council of the European Union.** (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Official Journal of the European Union, L 119, 1-88. https://eur-lex.europa.eu/eli/reg/2016/679/oj
- **Jara Valderrama, G.** (2018). *Protección de datos personales en Chile: Análisis y desafíos de la Ley 19.628 y su reforma*. Revista Chilena de Derecho y Tecnología, 7(1), 45-80.
- **McDermott, J.** (2017). *HIPAA Compliance Handbook*. Wolters Kluwer.
- **Ministerio del Interior y Seguridad Pública de Chile.** (2023). *Plan Nacional de Ciberseguridad 2023-2028*. https://ciberseguridad.gob.cl/pncs-2023-2028/
- **República de Chile.** (1999). *Ley de Protección de la Vida Privada (Ley No. 19.628)*. Biblioteca del Congreso Nacional de Chile. https://www.bcn.cl/leychile/navegar?idNorma=30590
- **Rojas Silva, P.** (2021). *El nuevo marco normativo de protección de datos personales en Chile: Comentarios a la propuesta de ley LPDP*. Revista de Derecho y Tecnologías de la Información, 10(2), 123-150.
- **Sáez García, L.** (2017). *La evolución de la protección de datos personales en Chile: De la Ley 19.628 a la propuesta de la nueva Ley LPDP*. Revista Iberoamericana de Protección de Datos, 5(3), 87-110.

- **Subsecretaría de Telecomunicaciones.** (n.d.). *Subsecretaría de Telecomunicaciones de Chile*. Gobierno de Chile. https://www.subtel.gob.cl/
- **U.S. Department of Health and Human Services.** (1996). *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
- **Voigt, P., & Von dem Bussche, A**. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer. doi:10.1007/978-3-319-57959-7