CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

Componentes Claves SGSI + SGIP

Ciclo de Workshops

ALIGNMENT
SOLUCIONES ESTRATÉGICAS

DIPLOMADO
CIBERSEGURIDAD

Agenda

- Introducción a los Sistemas de Gestión
- Componentes claves
  - Análisis del Contexto
  - Liderazgo
  - Planificación
  - Gestión de Riesgos
  - Recursos Generales
  - Operación
  - Mejora Continua

Profesor del Curso - Carlos Lobos de Medina

carlos.lobos@gmail.com

https://www.linkedin.com/in/clobos/

- Ingeniero Civil en Informática y Magister en Informática © de la Universidad de Santiago de Chile, Diplomado en Auditoría de Sistemas, Postitulado en Seguridad Computacional y Gestión de Procesos de Negocios de la Universidad de Chile.
- Especialista en gobernanza, gestión y control de tecnologías de información empleando modelos como COBIT, ITIL, ISO 27001 e ISO 22301. Posee certificaciones internacionales CISA, CISM, COBIT, ISO Lead Auditor 27001, ISO Lead Auditor BS 25599 e ITIL V3, entre otras.
- Director de los Programas de Ciberseguridad de Capacitación USACH.

Próximas actividades

MARTES 06 DE ENERO – 11:00 A 13:00 HRS (GMT-3 Hora Chile)

MIÉRCOLES 07 DE ENERO – 11:00 A 13:00 HRS (GMT-3 Hora Chile)

JUEVES 08 DE ENERO – 11:00 A 13:00 HRS (GMT-3 Hora Chile)

VIERNES 09 DE ENERO – 11:00 A 13:00 HRS (GMT-3 Hora Chile)

https://alignment.cl/programa-de-cumplimiento-digital/

Introducción

Sistemas de Gestión ISO 27001 + ISO 27701

- La ISO 27001 define los requisitos para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), es el estándar más utilizado a nivel global en la materia y se complementa con una gran cantidad de normas relacionadas.
- **Clave para la Implementación de Ley Marco de Ciberseguridad**
- Ultima versión: 2022

- La ISO 27701 define los requisitos para la implementación del Sistema de Gestión de Información de Privacidad (SGIP), es el estándar más utilizado a nivel global en la materia, siendo independiente de la ISO 27001 desde su última versión.
- **Clave para la Implementación de Ley Protección de Datos (RGPD)**
- Ultima versión: 2025

Definición de un SGSI

"Es un sistema que determina que requiere protegerse, y por qué, de que debe ser protegido y como protegerlo."

Albert, 2003

¿Que requiere protegerse?

- Los procesos de negocio
- La información y TIC habilitantes

¿por qué protegerlos?

- El valor que tienen para el negocio
- Para preservar la CID requerida

¿De qué protegerlos?

- Amenazas
- Vulnerabilidades

¿Cómo protegerlos?

- Con una metodología
- Con prácticas de gestión de riesgo
- Implementando controles
- Con un proceso estructurado
- Mejorando continuamente
- Competencias

Fuente: Managing Information Security Risk – Christopher Albert.2003

Podemos extenderlo a un SGIP

"Es un sistema que determina que requiere protegerse, y por qué, de que debe ser protegido y como protegerlo."

Albert, 2003

¿Que requiere protegerse?

- Los procesos de negocio
- **La información de carácter personal**
- TIC habilitantes

¿por qué protegerlos?

- El valor que tienen para el negocio
- **Cumplimiento normativo**
- Para preservar la CID requerida

¿De qué protegerlos?

- Amenazas
- Vulnerabilidades

¿Cómo protegerlos?

- Con una metodología
- Con prácticas de gestión de riesgo
- Implementando controles
- Con un proceso estructurado
- Mejorando continuamente
- Competencias

Fuente: Managing Information Security Risk – Christopher Albert.2003

Anexo SL – Estructura de Alto Nivel de los Sistemas de Gestión

✓Desde el año 2012 a la fecha la publicación de las normas ISOs que definen Sistemas de Gestión presenta una estructura común definida en el Anexo SL.

Clausula 1:	Objeto y campo de aplicación
Clausula 2:	Referencias normativas
Clausula 3:	Términos y definiciones
Clausula 4:	Contexto de la organización
Clausula 5:	Liderazgo
Clausula 6:	Planificación
Clausula 7:	Soporte
Clausula 8:	Operación
Clausula 9:	Evaluación del desempeño
Clausula 10:	Mejora

- ✓ Todas las normas ISO que definen sistemas de gestión tienen esta estructura.
- ✓ Son además las normas certificables.

Anexo SL – Estandarización de Sistemas de Gestión

Clausula 1:	Objeto y campo de aplicación
Clausula 2:	Referencias normativas
Clausula 3:	Términos y definiciones
Clausula 4:	Contexto de la organización
Clausula 5:	Liderazgo
Clausula 6:	Planificación
Clausula 7:	Soporte
Clausula 8:	Operación
Clausula 9:	Evaluación del desempeño
Clausula 10:	Mejora

Clausula	ISO 20.000	ISO 22.301	ISO 27.001
1	Objeto y ámbito de aplicación.		
2	Referencias normativas		
3	Terminología ISO 20.000-1	Terminología ISO 22.300	Terminología ISO 27.000
4	Contexto Interno y Externo, Partes Interesadas y Alcance		
5	Liderazgo, roles, responsabilidades y Política.		
6	Gestión de Servicios, Riesgos y Procesos.	Análisis de Riesgos, Análisis del Impacto en el Negocio y Planes de Continuidad	Gestión de Riesgos. controles y plan de tratamiento
7	Recursos, Competencia, Concienciación, Comunicaciones y Gestión Documental		
8	Operación del Sistema de Gestión (Implementación)		
9	Revisión de Objetivos, Auditoría Interna y Revisión de la Dirección		
10	Opciones de mejora, acciones correctivas → Mejora Continua		

Beneficios del Anexo SL

- ✓ La estandarización que poseen los sistemas de gestión facilita su adopción de manera integrada.

- ✓ Muchos son los beneficios de estos:
  - ✓ Desarrollar una política general única
  - ✓ Emplear un único sistema de gestión documental
  - ✓ Establecer mecanismos de revisión de la dirección integrado
  - ✓ Realizar auditorías conjuntas a los sistemas de gestión
  - ✓ Establecer mecanismos de mejora continua integrados
  - ✓ .....

- ✓ Hoy en día muchas organizaciones avanzan a:
  - ✓ ISO 9.000 + ISO 27.001 + ISO 27.701
  - ✓ ISO 9.000 + ISO 20.000
  - ✓ ISO 9.000 + ISO 27.001 + ISO 22.301
  - ✓ ISO 9.000 + ISO 20.000 + ISO 27.001

Características de la ISO 27701

1 Es un sistema de gestión certificable

Permite a las organizaciones obtener **certificación formal** de su cumplimiento en privacidad, mediante auditorías independientes, al igual que ISO 27001 en seguridad de la información.

> *Demuestra cumplimiento real, no solo declarativo.*

2 Alinea la gestión con el marco europeo (GDPR)

Recoge los **principios, derechos y obligaciones del Reglamento General de Protección de Datos (GDPR)**, asegurando equivalencia con estándares internacionales de privacidad.

> *Facilita interoperabilidad con Europa y otros mercados que reconocen el GDPR.*

3 Incorpora los principios universales de privacidad (ISO 29100)

Integra principios como **licitud, finalidad, minimización, exactitud, seguridad y responsabilidad demostrable**, transformándolos en políticas y controles concretos.

> *Conecta la ética de la privacidad con la gestión operativa.*

4 Establece roles y responsabilidades formales

Distingue y define los deberes del **responsable (PII Controller)** y del **encargado (PII Processor)**, creando claridad organizacional y fortaleciendo la rendición de cuentas.

> *Claridad de funciones = menos brechas y conflictos de control.*

5 Complementa, pero no depende, de ISO 27001 e ISO 27002

Aunque se origina en la familia de seguridad de la información, hoy actúa como **estándar autónomo**, manteniendo compatibilidad con sistemas de gestión de seguridad (SGSI).

> *Seguridad + Privacidad = Confianza digital institucional.*

6 Aporta trazabilidad y evidencia de cumplimiento (Accountability)

Exige **documentar políticas, evaluaciones de impacto, registros y decisiones**, asegurando que la organización pueda **probar cumplimiento** ante reguladores como la Agencia de Protección de Datos.

> *Lo que no se evidencia, no se cumple.*

7 Facilita la adecuación a leyes nacionales como la Ley 21.719

Sus controles y requisitos se alinean perfectamente con los **principios de la ley chilena**, proporcionando una **metodología estructurada** para implementarla de manera verificable.

> CL *La ISO 27701 es el puente entre la ley y la práctica.*

8 Es un estándar global y evolutivo

Reconocido a nivel internacional, su adopción demuestra **madurez institucional y compromiso con la privacidad**, y se actualiza para incorporar buenas prácticas emergentes (como IA y gobernanza de datos).

> *Garantiza competitividad y confianza en un ecosistema digital global.*

Principal cambio ISO 27701: Sistema de Gestión Independiente

ANTES

- Extensión de la ISO 27001 y 27002, mas un conjunto de controles adicionales propios de la información de privacidad.
- Se analizaba cada clausula de la ISO 27001 y en caso de ser necesario se establecían extensiones para privacidad.
- Se analizaba cada control de la ISO 27002 y en caso de ser necesario se establecían extensiones para privacidad.
- Definía una serie de controles propios para la privacidad.

HOY Versión 2025

- Sistema de Gestión de Información de Privacidad ISO 27701, en total autonomía y alineado todos los principios de un Sistema de Gestión
- Todas las clausulas del Sistema de Gestión son independientes y relativas a privacidad.
- Define controles propios para la información de privacidad

Similitudes: Ambos son Sistemas de Gestión

PLANIFICAR

- 4 CONTEXTO DE LA ORGANIZACIÓN
  - COMPRENSIÓN DE LA ORGANIZACIÓN Y SU CONTEXTO
  - COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS
  - DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE INFORMACIÓN DE PRIVACIDAD
  - SISTEMA DE GESTIÓN DE INFORMACIÓN DE PRIVACIDAD
- 5 LIDERAZGO
  - LIDERAZGO Y COMPROMISO
  - POLÍTICA DE PRIVACIDAD
  - ROLES, RESPONSABILIDADES Y AUTORIDADES
- 6 PLANIFICACIÓN
  - ACCIONES PARA ABORDAR LOS RIESGOS Y OPORTUNIDADES
  - OBJETIVOS DE PRIVACIDAD Y PLANIFICACIÓN PARA LOGRARLOS
  - PLANIFICACIÓN DE LOS CAMBIOS

HACER

- 7 APOYO
  - RECURSOS
  - COMPETENCIA
  - CONCIENCIZACIÓN
  - COMUNICACIÓN
  - INFORMACIÓN DOCUMENTADA
- 8 OPERACIÓN
  - PLANIFICACIÓN Y CONTROL OPERACIONAL
  - EVALUACIÓN DE RIESGSO DE PRIVACIDAD
  - TRATAMIENTO DE RIESGOS DE PRIVACIDAD

VERIFICAR

- 9 EVALUACIÓN DE DESEMPEÑO
  - SEGUIMIENTO, MEDICIÓN ANÁLISIS Y EVALUACIÓN
  - AUDITORÍA INTERNA
  - REVISIÓN POR LA DIRECCIÓN

ACTUAR

- 10 MEJORA
  - MEJORA CONTINUA
  - NO CONFORMIDAD Y ACCIONES CORRECTIVAS

Anexos de la ISO 27701

Anexo A (Normativo)

Objetivos de control de referencia y controles del Sistema de Gestión de Información de Privacidad (PIMS) aplicables a **responsables del tratamiento (PII Controllers)** y **encargados del tratamiento (PII Processors).**

> Este anexo establece los **controles mínimos obligatorios** que las organizaciones deben implementar para gestionar de manera segura, legal y responsable la información de identificación personal (PII).
> Define objetivos de control específicos en materia de consentimiento, derechos del titular, transparencia, transferencias internacionales, tratamiento de datos sensibles y retención limitada.

Anexo B (Normativo)

Guía de implementación para responsables y encargados del tratamiento de información personal (PII Controllers y PII Processors).

> Entrega **orientaciones prácticas y operativas** para aplicar los controles del Anexo A según el rol que cumple cada organización, su contexto, tamaño y nivel de madurez en privacidad.
> Incluye ejemplos de procedimientos, políticas internas y mecanismos de verificación para asegurar **trazabilidad y cumplimiento demostrable (accountability).**

Anexo C (Informativo)

Correspondencia con la norma ISO/IEC 29100 – Marco de Privacidad.

> Describe la relación directa entre los **principios de privacidad definidos en ISO/IEC 29100** (como limitación de propósito, minimización y responsabilidad) y los **controles operativos del PIMS.**
> Permite a las organizaciones mantener **consistencia conceptual** entre la gestión estratégica de la privacidad y su implementación práctica.

Anexo D (Informativo)

Correspondencia con el Reglamento General de Protección de Datos (GDPR) de la Unión Europea.

> Muestra cómo los controles y requisitos del PIMS **responden a los principios, derechos y obligaciones establecidos por el GDPR**, facilitando la armonización con marcos regulatorios internacionales.
> Destaca correspondencias clave como: base legal, consentimiento, evaluación de impacto, portabilidad, privacidad desde el diseño y supervisión de terceros.

Anexo E (Informativo)

Relación con las normas ISO/IEC 27018 e ISO/IEC 29151.

> Explica la complementariedad del PIMS con las normas especializadas en **protección de datos personales en entornos de nube pública (ISO 27018)** y **protección de información de identificación personal (ISO 29151).**
> Refuerza que, aunque la ISO/IEC 27701 ahora es independiente, **mantiene compatibilidad técnica** con los marcos de seguridad y confidencialidad derivados de la familia 27000.

Anexo F (Informativo)

Correspondencia con la versión anterior ISO/IEC 27701:2019.

> Detalla los **cambios estructurales, nuevas definiciones y controles actualizados** en la versión 2024, que consolida al PIMS como un **sistema de gestión autónomo** e independiente de ISO 27001/27002.
> Incluye ajustes terminológicos (PII Controller / Processor), la incorporación de nuevos roles de supervisión, y la ampliación del enfoque hacia **cumplimiento normativo y evaluación de impacto en privacidad (PIA).**

Actividades Claves desde el Sistema de Gestión

1 Contexto de la organización y partes interesadas

Identificar el entorno interno y externo, los actores involucrados (titulares, proveedores, reguladores) y los factores que afectan la gestión de la privacidad.

> 🌐 *Permite alinear el PIMS con los riesgos, objetivos y obligaciones reales de la institución.*

2 Liderazgo y compromiso de la alta dirección

La dirección debe **asumir responsabilidad y demostrar apoyo activo**, asignando recursos, roles y autoridad al sistema.

> 🏛️ *Sin liderazgo, no hay cultura de privacidad ni sostenibilidad del sistema.*

3 Política de privacidad institucional

Definir una política formal que refleje el compromiso con los **principios de protección de datos**, la **Ley 21.719**, el **GDPR** y los estándares internacionales.

> 📜 *La política es la carta magna del PIMS.*

4 Planificación y gestión del riesgo de privacidad

Identificar riesgos, establecer objetivos de privacidad y definir acciones preventivas y de mitigación.

> ⚖️ *Alinea la gestión con el principio de proporcionalidad y la mejora continua.*

5 Roles, responsabilidades y estructura organizacional

Designar funciones clave como el **Encargado de Protección de Datos (EPD)** y los responsables de tratamiento, estableciendo jerarquías y dependencias formales.

> 👥 *Claridad organizacional = rendición de cuentas efectiva.*

6 Soporte y recursos

Asegurar que el sistema cuente con **recursos humanos, tecnológicos y financieros** adecuados, junto con mecanismos de concienciación y formación permanente.

> 💡 *La privacidad no se declara: se sostiene con recursos.*

7 Control documental y operacional

Mantener y gestionar la documentación del PIMS: políticas, procedimientos, inventarios, evaluaciones de impacto y registros de tratamiento.

> 🗂️ *Evidencia tangible del cumplimiento (Accountability).*

8 Evaluación del desempeño y auditoría interna

Medir la eficacia del sistema mediante **indicadores, revisiones periódicas y auditorías internas**, reportando resultados a la alta dirección.

> 📊 *La mejora continua se construye sobre datos verificables.*

9 Mejora continua y acciones correctivas

Implementar un ciclo PDCA (**Planificar–Hacer–Verificar–Actuar**) que permita identificar no conformidades, analizarlas y fortalecer el sistema.

> 🔄 *Privacidad como proceso evolutivo, no estático.*

10 Integración con otros sistemas de gestión

El PIMS puede integrarse con **ISO 27001 (seguridad)**, **ISO 9001 (calidad)** o **ISO 37301 (compliance)**, generando sinergias de gobernanza.

> 🔗 *Un enfoque integrado reduce costos, brechas y duplicidades.*

Actividades Claves desde la Privacidad

1 **Identificación de roles y responsabilidades**

Definir claramente quién es el **Responsable del Tratamiento (PII Controller)** y quién actúa como **Encargado (PII Processor)** dentro de la organización.

> 👥 *Claridad de funciones = trazabilidad y rendición de cuentas.*

---

2 **Elaboración del inventario de tratamientos de datos personales**

Registrar todas las actividades de tratamiento, bases de datos, finalidades y flujos de información (internos y externos).

> 📋 *Base esencial para cumplir con la transparencia y el principio de finalidad.*

---

3 **Evaluación de riesgos de privacidad (Privacy Risk Assessment)**

Analizar riesgos asociados al tratamiento de datos personales e implementar controles proporcionales.

> ⚖️ *Permite priorizar recursos y adoptar medidas efectivas.*

---

4 **Evaluación de impacto en privacidad (PIA/DPIA)**

Realizar evaluaciones preventivas cuando el tratamiento pueda generar **alto riesgo para los derechos de las personas.**

> 🔍 *Requisito clave del GDPR y la Ley 21.719 para tratamientos sensibles o masivos.*

---

5 **Definición de políticas y procedimientos de privacidad**

Documentar políticas sobre **consentimiento, derechos ARCO+, conservación, eliminación, transferencia y brechas de seguridad.**

> 📄 *Convierte la normativa en procedimientos concretos y auditables.*

---

6 **Gestión de derechos del titular (ARCO+)**

Implementar canales formales para atender solicitudes de **acceso, rectificación, cancelación, oposición y portabilidad** de datos.

> ✉️ *Demuestra respeto activo al principio de participación individual.*

---

7 **Implementación de medidas técnicas y organizativas**

Aplicar controles de seguridad y privacidad como cifrado, anonimización, control de accesos, registros de actividad y segregación de funciones.

> 🔒 *Integración efectiva entre seguridad y privacidad.*

---

8 **Gestión de incidentes y brechas de datos personales**

Definir procedimientos de **detección, reporte, análisis y notificación** de incidentes ante la Agencia y los titulares afectados.

> 🚨 *Obligación crítica en el marco de la Ley 21.719.*

---

9 **Monitoreo, auditoría y mejora continua**

Evaluar periódicamente la eficacia del PIMS mediante auditorías internas y planes de acción.

> 📊 *El ciclo PDCA (Planificar–Hacer–Verificar–Actuar) mantiene la madurez y mejora del sistema.*

---

10 **Concienciación y formación institucional**

Capacitar al personal en los principios, procedimientos y responsabilidades del PIMS.

> 🎓 *La cultura organizacional es el control más eficaz de todos.*

¿Por qué implementar la Ley 21719 con la ISO 27701?

1. **Transforma el cumplimiento en gestión proactiva**
ISO 27701 permite pasar del cumplimiento reactivo ante fiscalizaciones a un modelo **preventivo y medible**, basado en riesgos, políticas y evidencia verificable ante la Agencia de Protección de Datos.

2. **Estructura la gobernanza de la privacidad**
Incorpora roles, responsabilidades y procesos claros para la gestión de datos personales, alineando áreas jurídicas, tecnológicas y de negocio bajo un **modelo de control integrado**.

3. **Asegura la trazabilidad y rendición de cuentas (accountability)**
Provee los **registros, métricas y controles** que exige la Ley 21.719 para demostrar cumplimiento frente a auditorías o requerimientos de la Agencia.

4. **Fortalece la gestión de riesgos de privacidad**
Permite identificar, evaluar y tratar los riesgos sobre datos personales con criterios objetivos, fortaleciendo la **cultura de gestión preventiva** y la toma de decisiones informadas.

5. **Integra la protección de datos al SGSI existente (ISO 27001)**
Evita duplicidades al complementar el sistema de seguridad de la información con un **módulo de privacidad (PIMS)**, logrando eficiencia en gestión, auditoría y mejora continua.

6. **Facilita la adaptación a la normativa nacional e internacional**
Sus controles se alinean con los principios de la Ley 21.719, el GDPR y otros marcos globales, facilitando la **interoperabilidad normativa** y reduciendo costos de adecuación futura.

7. **Mejora la confianza institucional y reputacional**
Demostrar cumplimiento normativo mediante un estándar internacional **aumenta la credibilidad pública** y la confianza de los ciudadanos, socios y entes fiscalizadores.

8. **Impulsa la mejora continua y la madurez organizacional**
Incorpora el ciclo **Planificar–Hacer–Verificar–Actuar (PDCA)** aplicado a la privacidad, asegurando evolución sostenida del sistema y consolidando una **cultura organizacional de protección de datos.**

"Agrega un completo y robusto sistema de gestión para abordar la ley, basado en el ciclo PDCA, con enfoque en riesgos, que fortalece la gobernanza, trazabilidad y control interno, posibilitando la integración con otros sistemas de gestión"

Controles para los responsables del tratamiento de información personal

Cláusula ISO 27701	Descripción resumida del control	Ley 19.628 (vigente hasta 2026)	Ley 21.719 (vigencia desde 2026)
A.1.2.2	Identificar y documentar propósito	Art. 9: uso sólo para los fines para los cuales fueron recolectados.	Art. 3 b)–c): principio de finalidad y proporcionalidad.
A.1.2.3	Identificar base legal	Art. 4 inc. 1: sólo con ley o consentimiento.	Arts. 12–13: consentimiento u otras bases legales.
A.1.2.4	Cuándo y cómo obtener consentimiento	Art. 4 incisos 1–4: consentimiento escrito, informado y revocable.	Art. 12: consentimiento libre, informado, específico, inequívoco y revocable.
A.1.2.5	Obtener y registrar consentimiento	Art. 4: consentimiento escrito e informado.	Art. 12 inc. final: responsable debe probar licitud.
A.1.2.6	Evaluación de impacto en privacidad (EIPD)	No prevista expresamente.	Art. 14 quáter: protección desde el diseño y por defecto.
A.1.2.7	Contratos con encargados	Art. 8: mandato por escrito con condiciones de seguridad.	Art. 15 bis: encargado sólo puede tratar datos por instrucciones del responsable.
A.1.2.8	Corresponsables	No regulado.	Art. 15 bis: diferencia entre responsable y encargado; responsable define fines y medios.
A.1.2.9	Registros de tratamiento (ROPA)	Art. 5: debe dejarse constancia de requirente, motivo y tipo de datos transmitidos.	Art. 14 ter a), d), h), i): registro público de actividades de tratamiento.

Obligaciones frente a los titulares de la información personal

Cláusula ISO 27701	Descripción resumida del control	Ley 19.628 (vigente hasta 2026)	Ley 21.719 (vigencia desde 2026)
A.1.3.2	Obligaciones con titulares	Art. 12: derecho a información, rectificación, eliminación.	Art. 4: derechos ARCO+, personales e irrenunciables.
A.1.3.3	Información a titulares	Art. 3: informar carácter obligatorio y finalidad.	Art. 14 ter: política pública de tratamiento.
A.1.3.4	Proveer información accesible	Art. 12: informar procedencia, finalidad y destinatarios.	Art. 5: derecho de acceso con detalle de tratamiento.
A.1.3.5	Modificar o retirar consentimiento	Art. 4 inc. 4: revocable por escrito.	Art. 12: revocable en cualquier momento sin causa.
A.1.3.6	Derecho de oposición	Art. 3 inc. 2: oposición al uso para publicidad.	Art. 8: oposición general incluso en marketing directo.
A.1.3.7	Acceso, rectificación y supresión	Arts. 12–16: acceso, modificación, eliminación.	Arts. 4–11: acceso, rectificación, supresión, oposición, bloqueo, portabilidad.
A.1.3.8	Informar a terceros cambios	Art. 12 final: aviso a quienes recibieron datos.	Art. 6 inc. 2: comunicar rectificación a destinatarios.
A.1.3.9	Proveer copia / portabilidad	Art. 12: copia gratuita del registro.	Art. 9: derecho a portabilidad electrónica.
A.1.3.10	Gestionar solicitudes de derechos	Art. 16: respuesta en 2 días hábiles.	Arts. 10–11: respuesta en 30 días + prórroga; reclamo ante Agencia.
A.1.3.11	Decisiones automatizadas	No regulado.	Art. 8 bis: derecho a no ser objeto de decisiones automáticas.

Obligaciones frente a los titulares de la información personal

Cláusula ISO 27701	Descripción resumida del control	Ley 19.628 (vigente hasta 2026)	Ley 21.719 (vigencia desde 2026)
A.1.4.2	Limitación de recolección	Art. 9.	Art. 3 b)–c) y 14 quáter: minimización y privacidad por diseño.
A.1.4.3	Limitación del tratamiento	Art. 9.	Art. 3 b).
A.1.4.4	Exactitud y calidad	Art. 6: corrección de datos inexactos.	Art. 3 d): principio de calidad.
A.1.4.5	Minimización / seudonimización	Art. 6 y 9.	Art. 3 c) y f), 14 quinquies: seudonimización y cifrado.
A.1.4.6	Eliminación / anonimización	Art. 6.	Art. 3 c): supresión o anonimización al finalizar propósito.
A.1.4.7	Archivos temporales	Art. 6 (bloqueo).	Art. 8 ter (derecho de bloqueo).
A.1.4.8	Retención	Art. 6.	Art. 3 c) y 14 ter i): período de conservación.
A.1.4.9	Destrucción segura	Art. 6.	Art. 3 c).
A.1.4.10	Controles de transmisión	Art. 5.	Art. 14 quinquies: cifrado y trazabilidad.

Intercambio, transferencia y divulgación de información personal

Cláusula ISO 27701	Descripción resumida del control	Ley 19.628 (vigente hasta 2026)	Ley 21.719 (vigencia desde 2026)
A.1.5.2	Base para transferencias internacionales	Art. 5.	Art. 14 ter h): informar nivel de protección o garantías.
A.1.5.3	Países / organizaciones destino	Art. 5.	Art. 14 ter h): identificar destinatarios extranjeros.
A.1.5.4	Registro de transferencias	Art. 5.	Art. 14 ter d), h): registro público.
A.1.5.5	Divulgaciones	Art. 5.	Art. 26: transferencias internacionales.

Obligaciones frente a los titulares de la información personal

Cláusula ISO 27701	Descripción resumida del control	Ley 19.628 (vigente hasta 2026)	Ley 21.719 (vigencia desde 2026)
A.2.2.2	Acuerdo con cliente (responsable)	Art. 8: mandato por escrito con condiciones de seguridad.	Art. 15 bis: obligación contractual entre responsable y encargado.
A.2.2.3	Fines del encargado	Art. 8: actuar según mandato.	Art. 15 bis: sólo bajo instrucciones del responsable.
A.2.2.4	Uso para marketing	No previsto.	Art. 8: requiere consentimiento del titular.
A.2.2.5	Instrucción ilícita	Implícito.	Art. 15 bis inc. 2: informar instrucciones ilícitas del responsable.
A.2.2.6	Obligaciones del cliente	Implícito.	Art. 15 bis y 14 quáter: corresponsabilidad y seguridad desde el diseño.
A.2.2.7	Registros del tratamiento	Art. 5: constancia de requirente y propósito.	Art. 14 ter: registro público y documentación del tratamiento.
A.2.3.2	Atender derechos de titulares	Art. 12: derecho a información y eliminación.	Arts. 4–11 y 15 bis: el encargado asiste al responsable.
A.2.4.2	Archivos temporales	Art. 6 (bloqueo).	Art. 8 ter: suspensión temporal del tratamiento.
A.2.4.3	Eliminación al término del contrato	Art. 6: eliminación de datos caducos.	Art. 3 c) y 14 quinquies d): eliminación segura al finalizar el servicio.
A.2.4.4	Controles de transmisión	Art. 5.	Art. 14 quinquies: cifrado y trazabilidad.

Intercambio, transferencia y divulgación de información personal

Cláusula ISO 27701	Descripción resumida del control	Ley 19.628 (vigente hasta 2026)	Ley 21.719 (vigencia desde 2026)
A.2.5.2	Transferencias internacionales	Art. 5.	Art. 26: sólo con nivel adecuado o garantías.
A.2.5.3	Países destino	Art. 5.	Art. 26: identificación del destinatario.
A.2.5.4	Registro de divulgaciones	Art. 5.	Art. 26.
A.2.5.5	Notificación de requerimientos legales	Implícito.	Art. 14 quinquies: informar incidentes o requerimientos de acceso.
A.2.5.6	Divulgaciones legalmente vinculantes	Implícito.	Art. 26 inc. final: sólo si la ley extranjera lo exige y se informa a la Agencia.
A.2.5.7	Divulgación de subencargados	No previsto.	Art. 15 bis inc. 3: informar subencargados.
A.2.5.8	Contratación de subencargados	No previsto.	Art. 15 bis inc. 3: autorización previa y mismas obligaciones.
A.2.5.9	Cambios de subencargados	No previsto.	Art. 15 bis inc. 3: informar cambios al responsable.

Consideraciones de seguridad para los responsables y encargados del tratamiento

Cláusula ISO 27701	Descripción resumida del control	Ley 19.628 (vigente hasta 2026)	Ley 21.719 (vigencia desde 2026)
A.3.3	Política de seguridad de la información	Art. 11: responsable debe adoptar medidas de seguridad adecuadas.	Art. 14 quinquies: políticas de seguridad técnicas y organizativas basadas en riesgos.
A.3.4	Roles y responsabilidades de seguridad	Art. 11: deber general del responsable.	Art. 14 quinquies letras a)–b): roles y medios para mantener confidencialidad e integridad.
A.3.5	Clasificación de la información	No explícito (principio de proporcionalidad Art. 9).	Art. 14 quinquies: medidas acordes al riesgo; Art. 17: mayor protección a datos sensibles.
A.3.6	Etiquetado de información	No regulado.	Art. 14 quinquies letras a) y d): confidencialidad, integridad y disponibilidad.
A.3.7	Transferencia de información segura	Art. 5: registro del requirente y propósito.	Art. 14 quinquies letras c)–d): cifrado, trazabilidad y canales seguros.
A.3.8	Gestión de identidades y accesos	Implícito en Art. 11.	Art. 14 quinquies letras c)–f): autenticación, control de acceso y prevención de accesos no autorizados.
A.3.9	Revisión de derechos de acceso	Art. 11.	Art. 14 quinquies letra f): acceso restringido y revisiones periódicas.
A.3.10	Seguridad con proveedores y terceros	Art. 8: mandato por escrito con condiciones de seguridad.	Art. 15 bis inc. 3: encargado y subencargados deben cumplir medidas equivalentes.
A.3.11	Planificación de gestión de incidentes	No específico; se asume bajo Art. 11.	Art. 14 sexies: plan de respuesta y registro de vulneraciones.

Consideraciones de seguridad para los responsables y encargados del tratamiento

Cláusula ISO 27701	Descripción resumida del control	Ley 19.628 (vigente hasta 2026)	Ley 21.719 (vigencia desde 2026)
A.3.12	Respuesta a incidentes y brechas	No regulado.	Art. 14 sexies: obligación de notificar a la Agencia y a titulares.
A.3.13	Cumplimiento legal y contractual	Art. 11 y 16.	Art. 14 quinquies letras g)–i): cumplimiento, supervisión y registro de medidas.
A.3.14	Protección de registros (logs)	No regulado expresamente.	Art. 14 quinquies: mantener registros seguros y protegidos.
A.3.15	Revisión independiente de seguridad	No previsto.	Art. 14 quinquies letra j): revisión periódica de eficacia de medidas.
A.3.16	Cumplimiento con políticas internas	Implícito en deber de diligencia.	Art. 14 quinquies letra j): evaluación continua y auditorías.
A.3.17	Concientización y capacitación	No regulado.	Art. 14 quinquies letra k): programas de capacitación en protección de datos.
A.3.18	Acuerdos de confidencialidad	Art. 7: obligación de confidencialidad.	Art. 14 quinquies letra b): obligación de confidencialidad permanente.
A.3.19	Escritorio y pantalla limpia	No regulado.	Art. 14 quinquies letras d)–f): medidas físicas y organizativas de resguardo.
A.3.20	Seguridad en almacenamiento	Art. 11: medidas de seguridad adecuadas.	Art. 14 quinquies letras d) y f): seguridad de almacenamiento, cifrado y control de soportes.
A.3.21	Eliminación o disposición segura	Art. 6: eliminación de datos caducos.	Art. 3 c) y Art. 14 quinquies letra d): disposición segura de medios.

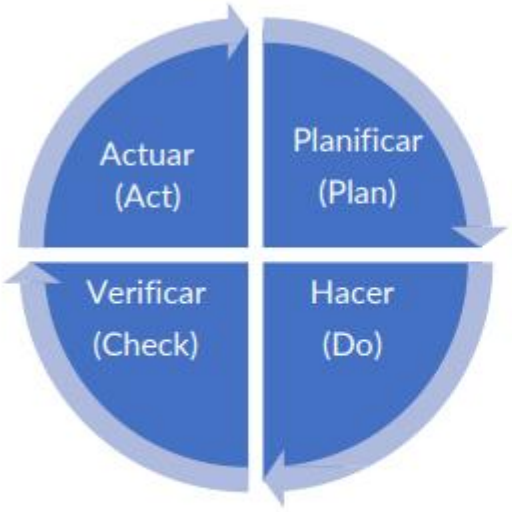
Consideraciones de seguridad para los responsables y encargados del tratamiento

Cláusula ISO 27701	Descripción resumida del control	Ley 19.628 (vigente hasta 2026)	Ley 21.719 (vigencia desde 2026)
A.3.22	Seguridad en dispositivos endpoint	No regulado.	Art. 14 quinquies letra f): evitar accesos no autorizados.
A.3.23	Autenticación segura	No regulado.	Art. 14 quinquies letra f): control de acceso y autenticación segura.
A.3.24	Respaldos y restauración	No regulado.	Art. 14 quinquies letra e): disponibilidad y resiliencia de sistemas.
A.3.25	Registro de eventos	No regulado.	Art. 14 quinquies letra i): trazabilidad de operaciones sobre datos.
A.3.26	Uso de criptografía	No regulado.	Art. 14 quinquies letra c): cifrado y seudonimización.
A.3.27	Desarrollo seguro de sistemas	No regulado.	Art. 14 quinquies letra j): revisión continua y control de cambios.
A.3.28	Requisitos de seguridad en aplicaciones	No regulado.	Art. 14 quinquies letra j): pruebas de eficacia de medidas.
A.3.29	Arquitectura e ingeniería segura	No regulado.	Art. 14 quáter: privacidad desde el diseño y por defecto.
A.3.30	Desarrollo tercerizado	Art. 8: condiciones contractuales al mandatario.	Art. 15 bis inc. 3: subencargados bajo mismas obligaciones.
A.3.31	Protección de información de pruebas	No regulado.	Art. 14 quinquies letras d) y f): proteger PII en entornos de prueba.

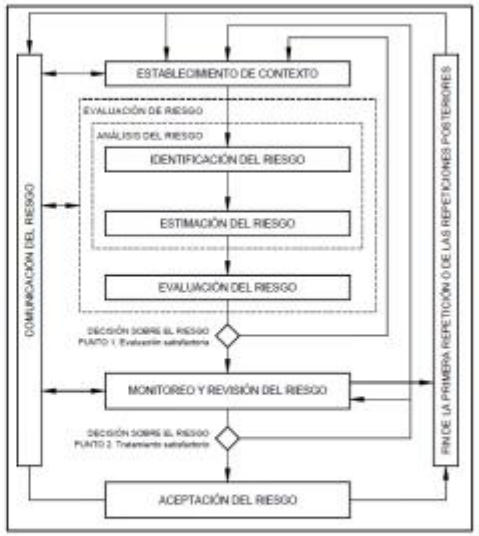
¿Que Ofrece ISO 27001?

Una metodología basada en mejores prácticas que posibilita la implementación de un SGSI

REQUISITO DE LA LEY
Implementar un Sistema de Gestión de Seguridad de la Información (SGSI)



Visión de Procesos alineada al ciclo PDCA



Enfoque de Riesgos

Controles de Seguridad de la Información

Clausula 1:	Objeto y campo de aplicación
Clausula 2:	Referencias normativas
Clausula 3:	Términos y definiciones
Clausula 4:	Contexto de la organización
Clausula 5:	Liderazgo
Clausula 6:	Planificación
Clausula 7:	Soporte
Clausula 8:	Operación
Clausula 9:	Evaluación del desempeño
Clausula 10:	Mejora

Metodología Estandarizada

Por diseño un SGSI mantiene un registro de acciones

REQUISITO DE LA LEY
Mantener un registro de las acciones ejecutadas del SGSI.

Procedimiento

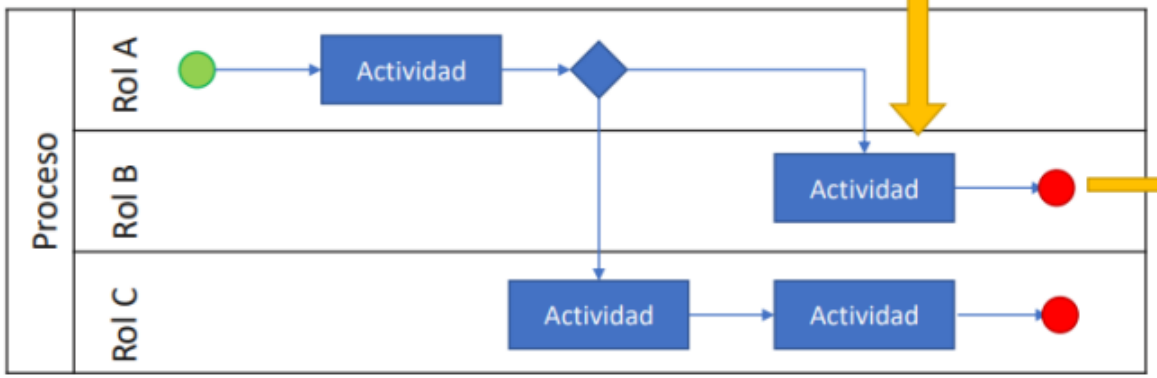
Describe como el proceso se lleva a cabo

Describe como desarrollar la actividad en especifico

Instructivo

Instructivo	
1	Paso 1
2	Paso 2
3	Paso 3
4	Paso 4
5	Paso 5

Proceso de Negocio (Qué, Quien, Cómo y Donde)



Registros
Presenta resultados obtenidos o evidencia de actividades

Un poco de Evolución

Fuente: Prestadores de Servicios Esenciales (PSE) y Operadores de Importancia Vital (OIV) Chiletec& Alt_Legal

Promulgación y Publicación de la Ley

DIARIO OFICIAL
DE LA REPUBLICA DE CHILE
Ministerio del Interior y Seguridad Pública

I SECCIÓN

LEYES, REGLAMENTOS, DECRETOS Y RESOLUCIONES DE ORDEN GENERAL

Núm. 43.820 | Lunes 8 de Abril de 2024 | Página 1 de 25

Normas Generales

CVE 2475674

MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA

LEY NÚM. 21.663

LEY MARCO DE CIBERSEGURIDAD

Teniendo presente que el H. Congreso Nacional ha dado su aprobación al siguiente

Proyecto de ley:

LEY 21663

EXPANDIR

- ENCABEZADO
- TÍTULO I DISPOSICIONES GENERALES
- TÍTULO II OBLIGACIONES DE CIBERSEGURIDAD
- TÍTULO III DE LA AGENCIA NACIONAL DE CIBERSEGURIDAD
- TÍTULO IV COORDINACIÓN REGULATORIA Y OTRAS DISPOSICIONES
- TÍTULO V DEL EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA DE LA DEFENSA NACIONAL
- TÍTULO VI DE LA RESERVA DE INFORMACIÓN EN EL SECTOR PÚBLICO EN MATERIA DE CIBERSEGURIDAD
- TÍTULO VII DE LAS INFRACCIONES Y SANCIONES
- TÍTULO VIII DEL COMITÉ INTERMINISTERIAL SOBRE CIBERSEGURIDAD
- TÍTULO IX ÓRGANOS AUTÓNOMOS CONSTITUCIONALES
- TÍTULO X DE LAS MODIFICACIONES A DIVERSOS CUERPOS LEGALES
- DISPOSICIONES TRANSITORIAS
- PROMULGACIÓN
- ANEXO PROYECTO DE LEY QUE ESTABLECE UNA LEY MARCO SOBRE CIBERSEGURIDAD E INFRAESTRUCTURA CRÍTICA DE LA INFORMACIÓN, CORRESPONDIENTE AL BOLETÍN N° 14.847-06

LEY 21663 | LEY MARCO DE CIBERSEGURIDAD

MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA

Generar url corta

Promulgación: 26-MAR-2024

Publicación: 08-ABR-2024

Versión: Última Versión - 01-MAR-2025

Materias: Ciberseguridad, Organismos Estatales, Organismos del Estado, Agencia Nacional de Ciberseguridad (ANCI)

Resumen: La presente ley tiene por objeto regular la normativa general aplicable a las acciones de ciberseguridad de l ... **ver más >>**

MODIFICACION | CONCORDANCIA | REGLAMENTO

Buscar en Norma

[Ley Chile - Ley 21663 - Biblioteca del Congreso Nacional]

Entidades Obligadas

- Dos clases de sujetos o entidades poseen obligaciones con esta ley:
  - Prestadores de Servicios Esenciales
  - Operadores de Importancia Vital
- Los prestadores de Servicios Esenciales se definen a nivel de sectores industriales
- Operadores de Importancia Vital se definen bajo definiciones y reglamentación asociada.
- No son necesariamente los mismos.

Quienes son Servicios Esenciales?

Los organismos de la Administración del Estado, tales como:

- Ministerios.
- Delegaciones Presidenciales Regionales y Provinciales.
- Gobiernos Regionales.
- Municipalidades.
- Fuerzas Armadas.
- Fuerzas de Orden y Seguridad Pública.
- Empresas públicas creadas por ley.
- Órganos y servicios públicos creados para el cumplimiento de la función administrativa.

El Coordinador Eléctrico Nacional.

Los prestadores bajo concesión de servicio público.

(*) El Senado y la Cámara de Diputados, el Poder Judicial, la Contraloría General de la República, el Banco Central, el Ministerio Público, el Servicio Electoral y el Consejo Nacional de Televisión, **no** están sujetos en modo alguno a la regulación, fiscalización o supervigilancia de la Agencia, pero deben tomar medidas de seguridad y coordinar reportes.

Fuente: Prestadores de Servicios Esenciales (PSE) y Operadores de Importancia Vital (OIV) Chiletec& Alt_Legal

Quienes son Servicios Esenciales?

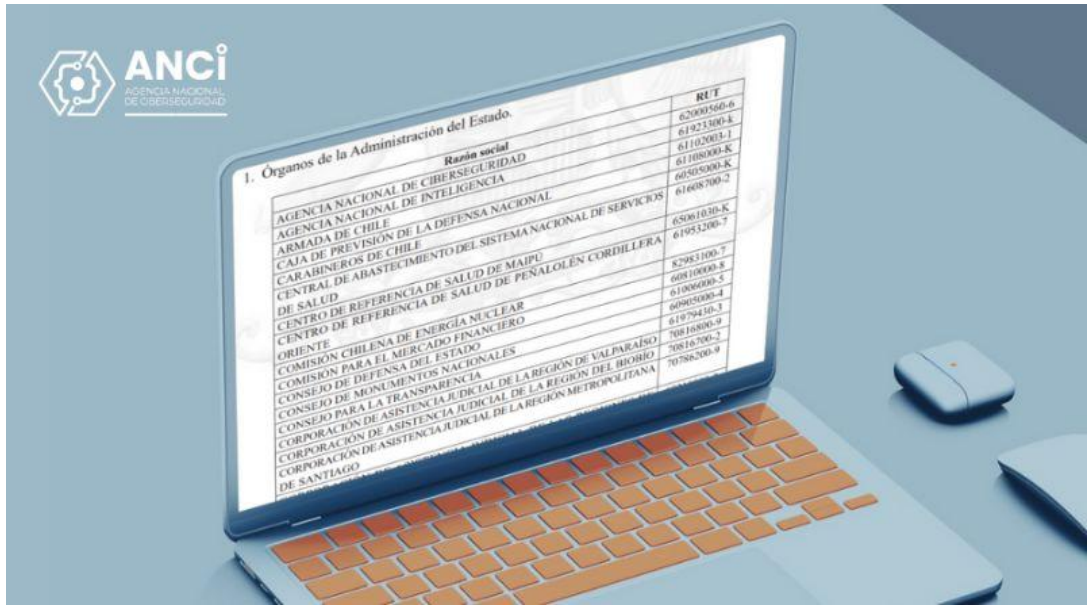
...por **instituciones privadas** que realicen las siguientes actividades:

- Generación, transmisión o distribución eléctrica
- Transporte, almacenamiento o distribución de combustibles.
- Suministro de agua potable.
- Saneamiento de agua potable.
- Telecomunicaciones.
- Transporte terrestre.
- Transporte aéreo.
- Transporte ferroviario
- Transporte marítimo.
- La operación de la infraestructura de las actividades de transporte.
- Banca, servicios financieros y medios de pago.
- Administración de prestaciones de seguridad social.
- Servicios postales y de mensajería.

Fuente: Prestadores de Servicios Esenciales (PSE) y Operadores de Importancia Vital (OIV) Chiletec& Alt_Legal

Operadores de Importancia Vital

- Son aquellas Prestadores de Servicios Esenciales u otras instituciones, cuya materialización de un incidente pueden afectar en:
- La seguridad y orden publico
- La prestación continua de servicios esenciales
- El cumplimiento de funciones del Estado
- El abastecimiento yo producción estratégica



https://www.diariooficial.interior.gob.cl/publicaciones/2025/09/16/44252/01/2699936.pdf

Operadores de Importancia Vital - Ejemplos

1. Órganos de la Administración del Estado.

Razón social	RUT
AGENCIA NACIONAL DE CIBERSEGURIDAD	62000560-6
AGENCIA NACIONAL DE INTELIGENCIA	61923300-k
ARMADA DE CHILE	61102003-1
CAJA DE PREVISIÓN DE LA DEFENSA NACIONAL	61108000-K
CARABINEROS DE CHILE	60505000-K
CENTRAL DE ABASTECIMIENTO DEL SISTEMA NACIONAL DE SERVICIOS DE SALUD	61608700-2
CENTRO DE REFERENCIA DE SALUD DE MAIPÚ	65061030-K
CENTRO DE REFERENCIA DE SALUD DE PEÑALOLÉN CORDILLERA ORIENTE	61953200-7
COMISIÓN CHILENA DE ENERGÍA NUCLEAR	82983100-7
COMISIÓN PARA EL MERCADO FINANCIERO	60810000-8
CONSEJO DE DEFENSA DEL ESTADO	61006000-5
CONSEJO DE MONUMENTOS NACIONALES	60905000-4
CONSEJO PARA LA TRANSPARENCIA	61979430-3
CORPORACIÓN DE ASISTENCIA JUDICIAL DE LA REGIÓN DE VALPARAÍSO	70816800-9
CORPORACIÓN DE ASISTENCIA JUDICIAL DE LA REGIÓN DEL BIOBÍO	70816700-2
CORPORACIÓN DE ASISTENCIA JUDICIAL DE LA REGIÓN METROPOLITANA DE SANTIAGO	70786200-9
CORPORACIÓN DE ASISTENCIA JUDICIAL DE LAS REGIONES DE TARAPACÁ Y ANTOFAGASTA	60318000-3
CORPORACIÓN NACIONAL DE DESARROLLO INDÍGENA	72396000-2
DEFENSA CIVIL DE CHILE	61109000-5
DEFENSORÍA DE LOS DERECHOS DE LA NIÑEZ	62000410-3
DEFENSORÍA DEL CONTRIBUYENTE	62000930-K
DEFENSORÍA PENAL PÚBLICA	61941900-6
DIRECCIÓN DE COMPRAS Y CONTRATACIÓN PÚBLICA	60808000-7
DIRECCIÓN DE EDUCACIÓN PÚBLICA	65154016-K
DIRECCIÓN DE PRESUPUESTOS	60802000-4
DIRECCIÓN DE PREVISIÓN DE CARABINEROS DE CHILE	61513000-1

3. Instituciones que proveen servicios de generación, transmisión o distribución eléctrica, y e Coordinador Eléctrico Nacional.

Razón social	RUT
ABASTIBLE S.A.	91806000-6
AELA GENERACIÓN S.A.	76489426-K
AES ANDES S.A.	94272000-9
ALBA SPA	76114239-9
ALBEMARLE LIMITADA	85066600-8
ALFA TRANSMISORA DE ENERGÍA S.A.	77337345-0
ALTO JAHUEL TRANSMISORA DE ENERGÍA S.A.	76100121-3
ALTO MAIPO SPA	76170761-2
AMANECER SOLAR SPA	76273559-8
ANA MARÍA S.A.	77677302-6
ANDES GENERACIÓN SPA	76203788-2
ANDES SOLAR II SPA	77423682-1
ANDES SOLAR IV SPA	76625173-0
ANDINA SOLAR 2 SPA	76466311-K
ANGLO AMERICAN SUR S.A.	77762940-9
ARAUCO BIOENERGÍA SPA	96547510-9
ARCADIA GENERACIÓN SOLAR S.A.	77696828-5
ASESORÍAS G-51 SPA	76105907-6
ASOC. DE CANAL. SOCIEDAD DEL CANAL DE MAIPO	70009410-3
AUSTRIANSOLAR CHILE CUATRO SPA	76337593-5
AUSTRIANSOLAR CHILE SEIS SPA	76362257-6
AVENIR SOLAR ENERGY CHILE SPA	76237387-4
BESALCO ENERGÍA RENOVABLE S.A.	76249099-4
BESALCO TRANSMISIÓN SPA	76975911-5
BIO ENERGÍA LOS PINOS SPA	76472359-7
BIO ENERGÍA MOLINA SPA	76256837-3
BIOENERGÍAS FORESTALES SPA	76188197-3
BLUE SOLAR CINCO SPA	76972749-3
BLUE SOLAR DOCE SPA	77157744-K
BLUE SOLAR OCHO SPA	77157648-6
BLUE SOLAR UNO SPA	76972735-3

4. Instituciones que proveen servicios de telecomunicaciones.

Razón social	RUT
AUSTRO INTERNET S.A.	78872080-7
BLUE TWO CHILE S.A.	99505690-9
CIRION TECHNOLOGIES CHILE S.A.	96896440-2
CLARO CARRIER S.A.	76654560-2
CLARO CHILE SPA.	96799250-K
CLARO COMUNICACIONES SPA	94675000-K
CLARO COMUNICACIONES SPA	96856970-8
CLARO SERVICIOS EMPRESARIALES S.A.	95714000-9
CLARO SERVICIOS S.A.	88381200-K
COMPAÑIA CHILENA DE COMUNICACIONES PARALLEL S.A.	99588540-9
COMPAÑIA DE TELEFONOS DE COYHAIQUE S.A.	92047000-9
COMPAÑIA NACIONAL DE TELEFONOS TELEFONICA DEL SUR S.A.	90299000-3
COMUNICACION Y TELEFONIA RURAL S.A.	96756060-K
COMUNICACIONES NETGLOBALIS S.A.	96964510-6
CTR Chile Networks S.A.	99560050-1
DB Terra Chile Holdco SpA	77494541-5
EMPRESA NACIONAL DE TELECOMUNICACIONES S.A.	92580000-7
ENTEL PCS TELECOMUNICACIONES S.A.	96806980-2
ENTEL TELEFONIA LOCAL S A	96697410-9
FULLCOM TELECOMUNICACIONES SPA	96527020-5
GALLYAS TELECOM S.A.	79913320-2
GTD Larga Distancia S.A.	96894200-K
GTD Manquehue Larga Distancia S.A.	96728540-4
GTD Manquehue S.A.	93737000-8
GTD METROCOM S.A.	96790850-9
GTD TELEDUCTOS S.A.	88983600-8
GTD Telesat S.A.	96721280-6
INGBELL CHILE SPA	76452881-6
INTERSUR LIMITADA	76500028-9
MI INTERNET SPA	76496622-8
NETLINE MOBILE S.A.	76660000-K
NETLINE TELECOMUNICACIONES CHILE S.A.	96921200-5
NOMADE TELECOMUNICACIONES S.A.	76355720-0
Pacífico Cable Spa	96722400-6

Operadores de Importancia Vital - Plazos

Fuente: Prestadores de Servicios Esenciales (PSE) y Operadores de Importancia Vital (OIV) Chiletec& Alt_Legal

Obligaciones para los PSE y OIV

- **Implementar** un Sistema de Gestión de Seguridad de la Información (SGSI) continuo.
- **Mantener** un registro de las acciones ejecutadas del SGSI.
- **Elaborar** e implementar planes de continuidad operacional y ciberseguridad.
- **Adoptar** de forma oportuna medidas para reducir el impacto y la propagación de un incidente de ciberseguridad
- **Contar** con un programa de formación y educación continua
- **Designar** un delegado de ciberseguridad, quien actuará como contraparte de la Agencia.
- **Reportar** los incidentes de ciberseguridad en los plazos exigidos
- **Certificación** del SGSI

Esto es solo aplicable a los Prestadores de Servicios Esenciales

Obligaciones para los PSE y OIV

	Servicios Esenciales	Operador de Importancia Vital
Deberes Generales	X	X
Deber de Reportar	X	X
Sistema de Gestión de Seguridad de la Información		X
Registro de las acciones ejecutadas SGSI		X
Planes de continuidad operacional y ciberseguridad		X
Revisión, ejercicios, simulacros y análisis de las redes.		X
Adoptar medidas necesarias para reducir el impacto.		X
Informar a los potenciales afectados		X
Contar con programas de capacitación, formación y educación continua		X
Designar un delegado de ciberseguridad		X

Charla ANCI: "Operadores de Importancia Vital (OIV): Etapas del proceso de calificación" (10 07 25)

Controles de Seguridad de la Información – Visión General

CIS Controls Version 8

Inventario y Control de los Activos Empresariales
Inventario y Control de Activos de Software
Protección de los Datos
Configuración Segura de Activos y Software Empresarial
Administración de Cuentas
Gestión de Control de Accesos
Gestión Continua de Vulnerabilidades
Gestión de Registros de Auditoría
Protección del Correo Electrónico y Navegador Web
Defensas contra Malware
Recuperación de Datos
Gestión de la Infraestructura de Red
Monitoreo y Defensa de la red
Concientización en Seguridad y Formación de Habilidades
Gestión de Proveedores de Servicios
Seguridad en el Software de Aplicación
Gestión de Respuesta a Incidentes
Pruebas de Penetración

ISO 27002:2022 Controles de Seguridad de la Información

Gobernanza
Gestión de Activos
Protección de Información
Seguridad en Recursos Humanos
Seguridad Fisica
Seguridad en Sistemas y Redes
Seguridad en Aplicaciones
Seguridad en la Configuración
Gestión de Identidades y Accesos
Gestión de Amenazas y Vulnerabilidades
Continuidad del Negocio
Seguridad en las Relaciones con Proveedores
Legal y Cumplimiento
Gestión de Eventos de Seguridad de la Información
Aseguramiento de la Seguridad de la Información
Inteligencia de Amenazas
Seguridad en la Nube
Privacidad y protección de PII
Gestión de Proyectos
Protección de Información

NIST SP 800-53 Revision 5

Control de Accesos
Concientización y Entrenamiento
Auditoría y Accountability
Evaluación, Autorización y Monitoreo de la Seguridad
Gestión de la Configuración
Planificación de la Contigencia
Identificación y Autenticación
Respuesta a Incidentes
Mantención
Protección de Medios
Protección Fisica y del Entorno
Planificación
Gestión del Programa
Seguridad del Personal
Transparencia y Procesamiento de PII
Evaluación de Riesgos
Adquisición de Sistemas y Servicios
Protección de Sistemas y Comunicaciones
Integridad de la Información y Sistemas
Gestión de Riesgos en la Cadena de Suministros

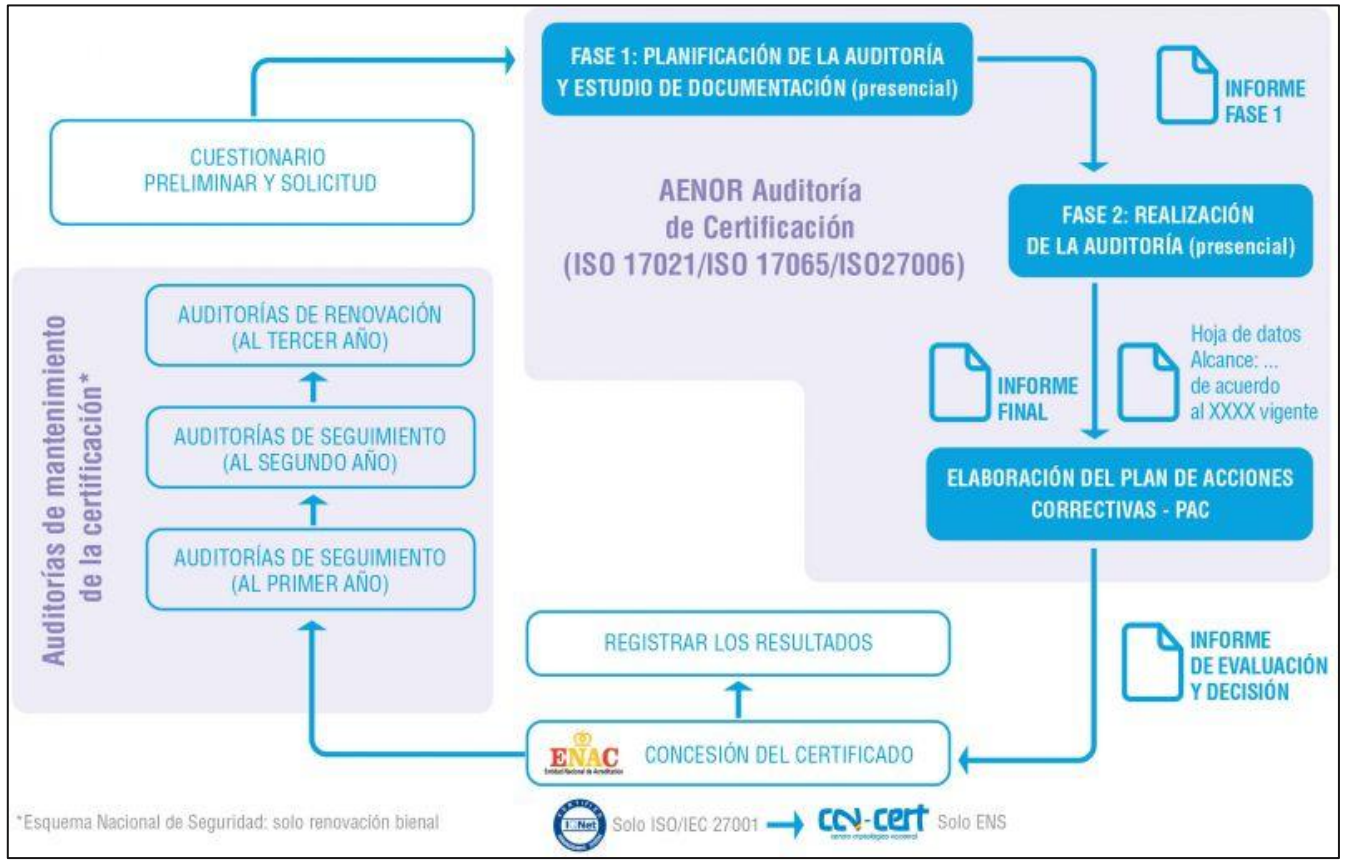
Controles de Seguridad de la Información – Visión General

Gobernanza	Gestión de Proyectos	Gestión de Activos	Control de Accesos	Seguridad en RRHH	Capacitación y Concientización	Protección de Información y Medios	Seguridad Física
Seguridad en la Configuración	Seguridad Operaciones	Gestión de Vulnerabilidades	Seguridad en Redes	Seguridad en Software	Seguridad con Proveedores	Gestión de la Continuidad	Gestión de Incidentes
Ciberinteligencia	Riesgos en Cadena de Suministro	Privacidad y Cumplimiento	Pentesting	Monitoreo Red y Servicios	Seguridad en la Nube	Auditoría y Aseguramiento	Gestión de Logs y Evidencia

Controles Administrativos Controles en TI Controles Ciber

#01	La implementación del SGSI no sólo involucra a TI, deber ser abordado desde una perspectiva integral y con buenas prácticas de gestión

Proceso de Certificación



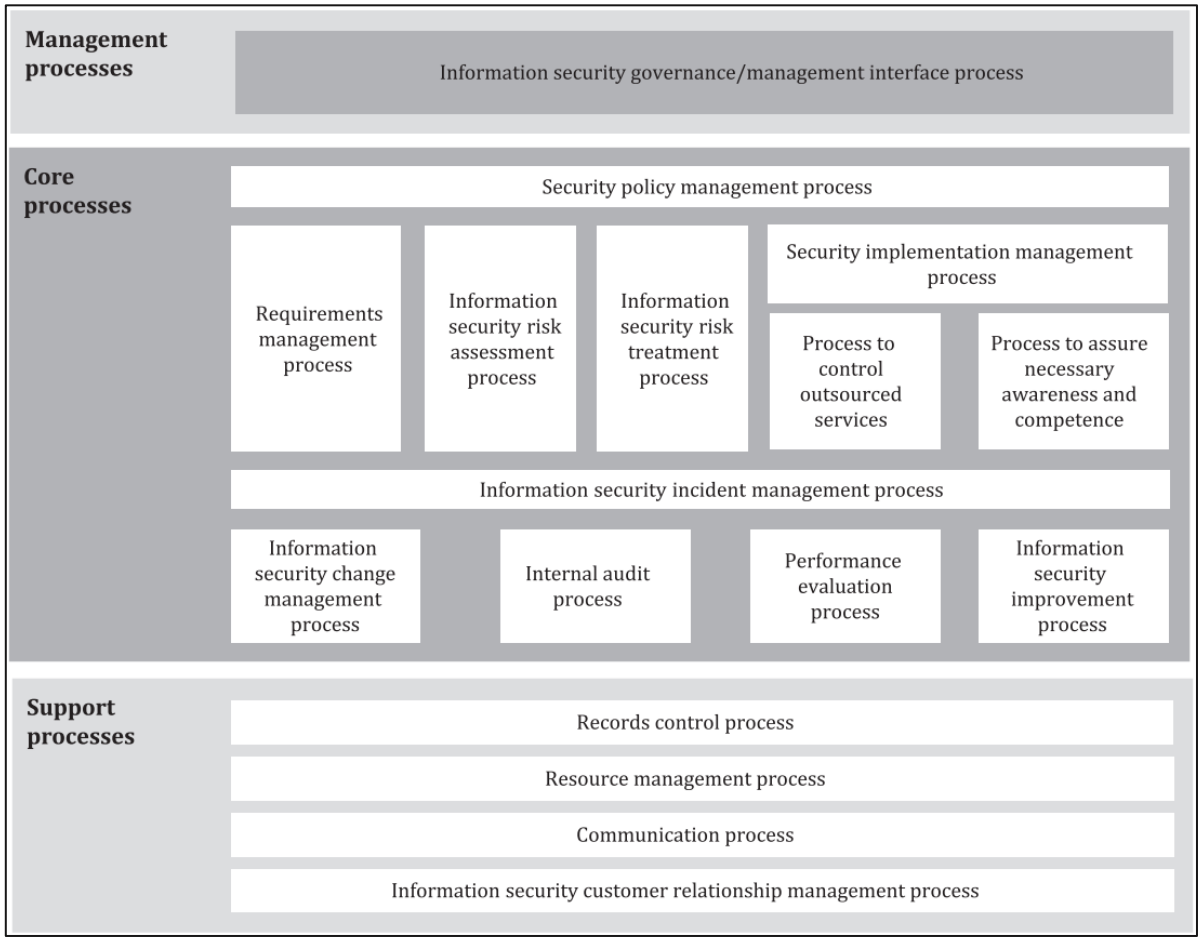
Los estándares ISO 27001 e ISO 27701 son los únicos certificables como Sistema de Gestión en Seguridad de la Información e Información de Privacidad respectivamente.

La visión miope de algunos "Expertos en Civerceguridad"

- ✓ Visión de "Experto de Ciberseguridad"
  - ✓ La verdadera ciberseguridad esta en las tecnologías y tener gente capacitada → Requiere Gobernanza, Procesos, Tecnologías, Herramientas, Personas y Recursos
  - ✓ La ciberseguridad debe basarse en el comportamiento del adversario (TTP) → Debe ser parte integral de la Gestión de Riesgos, así la Inteligencia de Amenazas, ambas incluidos en la ISO 27001/27002
  - ✓ La ISO 27001 no sirve para nada, es solo para documentar y demostrar cumplimiento → Requiere formalizar tus políticas, procedimientos y acciones, posibilitando demostrar el cumplimiento con reguladores y clientes.
  - ✓ La ISO 27001 es un estándar de seguridad no tiene nada que ver con ciberseguridad → La ciberseguridad es un subconjunto de la seguridad de la información, la profundidad en la cual se implementa marca la diferencia.
  - ✓ La ISO 27001 no garantiza la ciberseguridad incluso estando certificado → ¿Qué herramienta,, norma o persona puede garantizar que una organización no sea atacada?

Sistema de Gestión ISO 27001 + ISO 27701

Procesos de un SGSI – ISO 27.022 (Serán extensibles a ISO 27701)



¡¡¡Parece que acá ya se complicó la cosa!!!

- Existen decisiones estratégicas que tomar?
- Tenemos que tener políticas de seguridad?
- Debemos gestionar nuestros riesgos?
- Habrá que controlar los servicios?
- Tenemos que capacitar a nuestros RRHH?
- Que hacer con las incidencias?

Parece que algunos procesos hay que tener!!!

- Si los procesos cambian?
- Necesitamos auditar los procesos?
- Evaluaremos los procesos?
- Será necesario irlos mejorando?

Necesitamos información para todo esto!!!

Visión de Procesos del SGSI – ISO 27022

Necesitamos 16 procesos para solo implementar el core del SGSI?

Cuantos procesos más serán necesarios para la implementación de controles?

No será demasiada documentación?

Será fácil de implementar de esta forma?

Otra forma de verlo

Procesos de Gestión

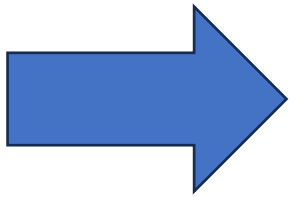
Procesos Core

Procesos de Soporte

Es fácil de implementar si entendemos y articulamos conceptos claves.

¿Como avanzar de manera agil?

- Entendiendo lo que se debe hacer en un SGSI
  - Comprensión de las clausulas
  - Comprensión de los entregables relacionados
  - Competencias de personas
- Definiendo roles y responsabilidades
  - A nivel de clausulas
  - A nivel de actividades
- Estableciendo definiciones simples de un proceso
  - Roles que entiendas su responsabilidad
  - Responsabilidades con capacidades asociadas
  - Entregables con responsabilidades clares



OBJETIVO:

Implementar los requisitos de la norma

Ejemplo 1: Analisis del Contexto

Clausula	Requisito	Actividad requerida	Medios de Verificación
4.1	Comprensión de la organización y de su contexto	La organización determina cuestiones externas e internas relevantes para su propósito y que afectan su capacidad para lograr los resultados previstos del sistema de gestión de seguridad de la información (SGSI)	Contexto Externo: - Análisis PESTEL Contexto Interno: - Análisis Estratégico - Análisis FODA - Análisis Arquitectura Empresarial - Análisis de Riesgos (Alto Nivel) - Análisis GAP

Debo describir en mi proceso como realizo las actividades específicas asociados a los entregables (Medios de Verificación)?

Analisis PESTEL – Análisis Externo

P	E	S	T	E	L
Institucionalidad	Aumentos de Precios de Servicios	Mayor uso de teléfonos, internet, redes sociales....	Riesgos en el sector	Gestión de residuos	Ley Marco de Ciberseguridad
Prioridades legislativas	Aumento de Rentas en Ciberseguridad	Mayor uso de tramites TICs en el Estado	Riesgos en las tecnologías claves	Eficiencia energética	Ley de Protección de Datos
Consideraciones presupuestarias	Rentas poco competitivas en el Sector Publico	Mayor valor en la protección de datos	Tendencias, desafíos y oportunidades	Riesgos ambientales derivados de ciberataques	Ley de Delitos Informáticos
Requisitos para el Sector	Inflación/Tasas de Cambio	Percepción de inseguridad	Herramientas de protección y arquitecturas de seguridad		Leyes sectoriales

Comprender el Estado Actual – Análisis Interno

Uso de Check List

CMMC Levels, Processes and Practices

Uso de Modelos de Madurez

Estudios Comparativos

Comprender el Estado Actual – Análisis Interno

Clausula 4: Análisis del Contexto ISO 27701

1. Identificar el contexto externo relacionado con privacidad

- Ley 21.719 y regulaciones sectoriales.
- ANPD (futura Autoridad Nacional) y requisitos de reporte.
- Normas internacionales (GDPR, 29100, 27018).
- Riesgos sociales, tecnológicos y culturales que afecten el tratamiento de PII.

2. Analizar el contexto interno de la organización

- Estructura, gobernanza y modelo de operación.
- Estrategia organizacional y madurez en seguridad y privacidad.
- Procesos actuales de tratamiento de PII.
- Dependencias internas relevantes (TI, legal, operaciones, proveedores).

3. Identificar partes interesadas (internas y externas)

- Titulares de datos.
- Autoridades reguladoras.
- Clientes, proveedores, socios de negocio y subencargados.
- Áreas internas que crean o consumen PII.

  → Documentar: necesidades, expectativas y requisitos de cada parte.

4. Determinar requisitos legales, contractuales y normativos

- Ley 21.719 y obligaciones asociadas (bases legales, derechos, principios).
- Contratos con encargados / subencargados.
- Políticas internas y compromisos con terceros.
- Estándares aplicables (ISO 27001, 27701, 29100, 27018).

5. Definir el alcance del PIMS (Privacy Information Management System)

- Qué actividades, procesos, unidades y tipos de PII están incluidos.
- Qué roles: Responsable, Encargado o ambos.
- Ubicaciones y sistemas involucrados.

  → El alcance debe declarar explícitamente la relación con ISO 27001.

6. Mapear procesos y actividades que tratan PII

- Inventario de procesos que generan, almacenan o comparten PII.
- Identificación de flujos de datos internos y externos.
- Clasificación inicial del tipo de PII según sensibilidad.

7. Identificar riesgos iniciales del contexto

- Riesgos derivados de cultura, tecnología, dependencia de terceros, etc.
- Riesgos regulatorios y reputacionales.

  → Estos serán entrada directa para la etapa de evaluación de riesgos del PIMS.

8. Validación con la Dirección

- Presentar el contexto, alcance, partes interesadas y requisitos.
- Ajustar decisiones estratégicas (rol de Responsable, Encargado, mixto).
- Obtener aprobación formal.

- Contexto interno y externo
- Partes interesadas y requisitos
- Requisitos legales y contractuales
- Inventario preliminar de procesos con PII
- Alcance del PIMS
- Entradas para la gestión de riesgos

Análisis del Contexto Externo e Interno

1. Marco regulatorio obligatorio y en expansión
Ley 21.719, Ley 21.180, Ley Marco de Ciberseguridad, Ley de Transparencia, directrices de Contraloría y normas sectoriales aplicables.

2. Fiscalización futura de la ANPD
Requisitos de registros, DPIA, evidencia de responsabilidad proactiva y notificación de incidentes de privacidad.

3. Interoperabilidad del Estado
Flujos de datos con otros organismos (Registro Civil, ChileAtiende, ClaveÚnica, ministerios), aumentando la superficie de riesgo de privacidad.

4. Expectativa ciudadana de transparencia y protección
Los ciudadanos demandan mayor control sobre su información y respuestas eficientes a solicitudes ARCO-

5. Riesgos sociales, tecnológicos y reputacionales
Filtraciones, ciberataques, incidentes públicos y presión mediática afectan la legitimidad institucional y la confianza pública.

1. Sistemas legacy y limitaciones tecnológicas
Plataformas antiguas sin trazabilidad, sin anonimización y con gestión limitada de retención/eliminación.

2. Fragmentación de roles y responsabilidades
Gestión dividida entre Jurídico, TI, Transparencia, Gestión Documental y áreas misionales, dificultando un PIMS coherente.

3. Entradas de datos masivos y sensibles
Programas sociales, subsidios, fichas, registros ciudadanos, atención pública: alto volumen y alta sensibilidad de PII.

4. Cultura organizacional centrada en cumplimiento administrativo
Predomina el foco en documentación y control formal por sobre la gestión de riesgos, dificultando la adopción del enfoque ISO 27701.

5. Limitaciones de recursos humanos y capacitación
Escasez de especialistas en privacidad, ciberseguridad y gobernanza, lo que impacta madurez, continuidad y sostenibilidad del PIMS.

"Comprender el contexto interno y externo es esencial en privacidad porque permite al organismo anticipar riesgos, alinear sus obligaciones legales y asegurar que cada decisión sobre datos personales responda a su realidad institucional y al entorno que la rodea."

Ejemplo 2: Analisis de Partes Interesadas

Clausula	Requisito	Actividad requerida	Medios de Verificación
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	La organización determina las partes interesadas relevantes para el SGSI y sus requisitos relevantes para la seguridad de la información	- Identificación de Partes Interesadas - Clasificación de Partes Interesadas - Mapas de relación Influencia/Interés - Requisito de Seguridad - Requisitos de Negocio - Requisitos de Servicios/Productos - Requisitos de Clientes - Requisitos de Reguladores - Mapeo de Requisitos con el SGSI

Debo describir en mi proceso como realizo las actividades específicas asociados a los entregables (Medios de Verificación)?

Análisis del Contexto: Partes Interesadas ISO 27701 (SP)

1. Ciudadanos y Beneficiarios

- Protección de sus datos y trato legítimo.
- Derechos ARCO+ claros y trazables.
- Transparencia en finalidades y uso.
- Expectativa de seguridad y confidencialidad.

2. Contraloría General de la República (CGR)

- Evidencia formal de cumplimiento.
- Procedimientos y actos administrativos controlados.
- Trazabilidad documental.
- Minimización y legalidad del tratamiento.

3. CAIGG (Consejo de Auditoría Interna General de Gobierno)

- Controles adecuados y coherentes.
- Gestión y registro de riesgos de privacidad.
- Evidencia útil para auditorías ministeriales.
- Alineamiento entre privacidad, control interno y ciberseguridad.

4. ANPD – Autoridad Nacional de Protección de Datos

(cuando entre en operaciones)

- Registro de tratamientos actualizado.
- DPIA para alto riesgo.
- Notificación oportuna de incidentes.
- Responsabilidad proactiva demostrable.

5. Otros Organismos Públicos (Interoperabilidad)

- Intercambio seguro y legítimo de datos.
- Finalidades explícitas y documentadas.
- Trazabilidad de flujos interinstitucionales.
- Minimización y proporcionalidad.

6. Proveedores Externos / Encargados del Tratamiento

- Contratos con cláusulas de privacidad robustas.
- Procesamiento bajo instrucciones formales.
- Notificación de incidentes.
- Seguridad equivalente o superior.

7. Funcionarios y Colaboradores

- Protección de su propia información.
- Capacitación en privacidad.
- Acceso restringido por función.
- Confidencialidad y uso adecuado de sistemas.

8. Dirección Superior / Alta Jefatura

- Reducción de riesgos reputacionales y regulatorios.
- KPIs y reportabilidad del PIMS.
- Integración en la estrategia institucional.
- Toma de decisiones basada en datos y riesgos.

Clausula Liderazgo – ISO 27001

Clausula	Requisito	Actividad requerida	Medios de Verificación
5.1	Liderazgo y Compromiso	La alta dirección demuestra liderazgo y compromiso con respecto al SGSI.	- Definición de objetivos - Plan de implementación - Presupuesto - Modelo de Gobernanza
5.2	Política	La alta dirección establece una política de seguridad de la información	- Política de Seguridad de la Información - Plan de comunicación y concientización
5.3	Roles, responsabilidades y autoridades organizacionales	La alta dirección asegura que las responsabilidades y autoridades para los roles relevantes para la seguridad de la información se asignen y se comuniquen en toda la organización.	- Organigrama - Modelo Roles y responsabilidades - Perfiles de Cargo Claves

El Liderazgo de un PIMS

1. Liderar con propósito institucional

Un jefe de servicio debe alinear cada proyecto, decisión y recurso con la misión pública y el impacto real en la ciudadanía.

2. Practicar la responsabilidad proactiva

No esperar a que surjan crisis. Anticiparse, monitorear riesgos y fortalecer procesos antes de que se transformen en problemas.

3. Gestionar con transparencia y rendición de cuentas

Comunicar decisiones, justificar prioridades y mostrar resultados medibles para generar confianza interna y ciudadana.

4. Fortalecer equipos y no solo funciones

Crear equipos interdisciplinarios, motivar, formar y empoderar a los funcionarios para que sean parte del cambio institucional.

5. Tomar decisiones basadas en evidencia

Usar datos, indicadores, auditorías, análisis de riesgo y desempeño para priorizar y asignar recursos estratégicamente.

6. Impulsar la innovación pública con prudencia

Promover la transformación digital, automatización y mejora continua, siempre cuidando seguridad, privacidad y legalidad.

7. Ser un puente entre lo técnico y lo político

Traducir temas complejos a un lenguaje claro para autoridades, equipos internos y ciudadanía, manteniendo coherencia y liderazgo.

8. Construir cultura institucional sólida

Fomentar valores de integridad, servicio público, respeto, colaboración, inclusión y protección de datos como eje de confianza estatal.

“En protección de datos, el liderazgo marca la dirección y la auditoría confirma el compromiso: solo una gestión que guía y verifica puede garantizar el cumplimiento real de la Ley 21.719 y la confianza de la ciudadanía.

Roles y Responsabilidades

🔵 1. Establecer un liderazgo formal y visible (Jefatura del Servicio)

La jefatura debe designar responsables, aprobar políticas, asignar recursos y comunicar que la privacidad es una prioridad institucional.
Sin liderazgo visible → el PIMS no avanza.

🔵 2. Crear un Comité de Privacidad y Protección de Datos

Debe integrar: Jurídico, TI, Transparencia, Gestión Documental, Unidades Misionales y Control Interno.
Este comité es clave para coordinar decisiones, aprobar procedimientos y definir riesgos.

🔵 3. Designar un Responsable de Privacidad / DPO interno

Puede estar en Jurídico o Contraloría Interna, con independencia operativa.
Rol clave: asesorar, revisar DPIA, coordinar acciones y ser intermediario con la ANPD.

🔵 4. Definir Encargados del Tratamiento en cada área

Cada área que trate PII debe tener un encargado responsable de:

- Inventario de datos
- Actualización de procesos
- Identificación de riesgos
- Respuesta a solicitudes ARCO+

Esto baja la responsabilidad al nivel operativo.

🔵 5. Crear un Equipo Técnico de TI para privacidad

Debe gestionar:

- Seguridad de la información
- Trazabilidad
- Minimización
- Controles de acceso
- Eliminación de datos
- Integración con ISO 27001/27002

Sin TI, la ley no se puede ejecutar.

🔵 6. Integrar a Control Interno y CAIGG

Control Interno debe verificar que políticas, DPIA, registros y procedimientos se cumplan.
Permite demostrar responsabilidad proactiva durante auditorías internas o ministeriales.

🔵 7. Definir responsables claros para ARCO+, incidentes y transparencia

Tres procesos críticos que deben tener dueños:

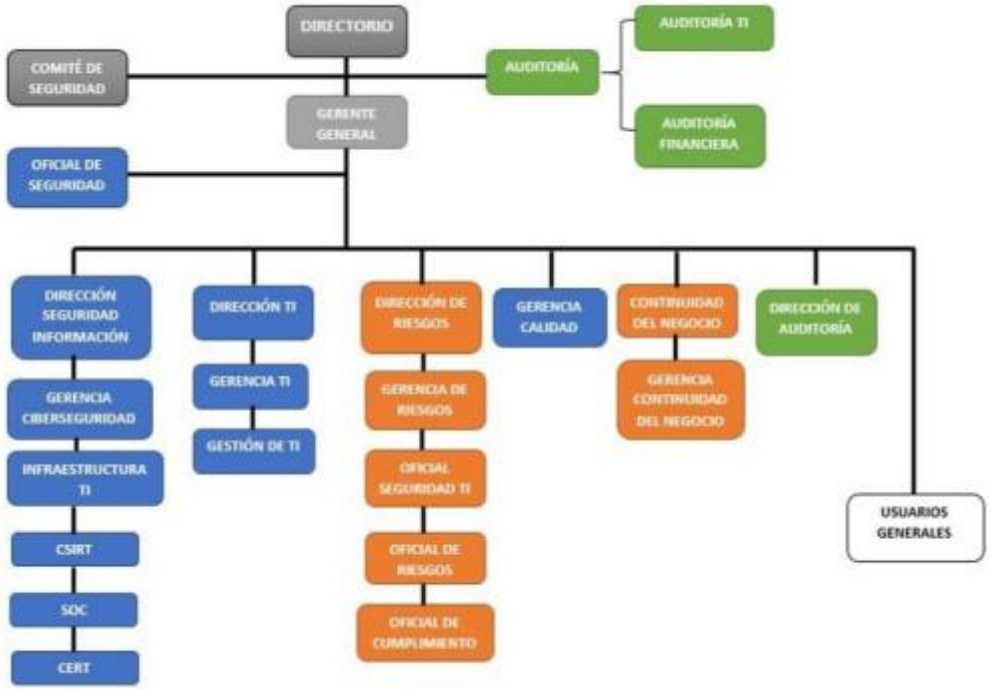
- **ARCO+:** Atención ciudadana / Jurídico
- **Incidentes de privacidad:** TI + Jurídico
- **Transparencia activa:** Gestión documental

Evita cuellos de botella y respuestas tardías.

🔵 8. Capacitar a todos los funcionarios según su rol

No basta con capacitar a TI o Jurídico.
Cada nivel debe saber **qué puede y no puede hacer con datos personales**, desde atención ciudadana hasta las jefaturas.
Capacitación + conciencia = reducción real del riesgo

Roles y Responsabilidades



Establezca son los roles y responsabilidades claves en las líneas de defensa, así como en cargos de responsabilidad especifica en SGSI y SGIP.

Política de Seguridad

Desde las buenas prácticas (ISO 27001/ISO 27002/ISO 27003)

Requisito	SI	NO
Es adecuada al propósito de la organización (misión/visión) ?		
Se alinea a la estrategia del negocio (Objetivos estratégicos) ?		
Incluye objetivos de seguridad de la Inf. o marco de referencia (Objetivos de SI)?		
Considera requisitos creados por la normativa, legislación y contratos?		
Considera el entorno actual y previsto de amenazas?		
Identifica y es representativa a las partes interesadas y sus requisitos?		
Es comunicadas a los empleados y terceras partes relevantes de una forma que sea apropiada, entendible y accesible ?		
Contiene la definición de la seguridad de la información, de sus objetivos y principios?		
Incluye el compromiso de cumplir con los requisitos aplicables a la Seguridad de la Inf.?		
Incluye el compromiso de mejora continua del SGSI?		

Clausula Planificación

Clausula	Requisito	Actividad requerida	Medios de Verificación
6.1	Acciones para tratar los riesgos y oportunidades	La organización define y aplica un proceso de evaluación y tratamiento de riesgos de seguridad de la información.	- Política de Gestión de Riesgos - Marco de Gestión de Riesgo - Proceso de Gestión de Riesgo - Matriz de Riesgos - Plan de Tratamiento de Riesgos - Declaración de Aplicabilidad de Controles (SoA)
6.2	Objetivos de seguridad de la información y planificación para su consecución	La organización establece objetivos de seguridad de la información y planea alcanzarlos en las funciones y niveles relevantes.	- Objetivos del SGSI - Mapa de KPI - Cuadro de Mando Integral - Plan de implementación - Proceso de Evaluación de Performance
6.3	Planificación de cambios	La organización realiza de manera planificada la implementación de cambios en el SGSI	- Proceso de Mejora Continua

Inventario de Activos

🔵 1. Identifica activos que "tratan" o "soportan" PII, no solo activos tecnológicos

Incluye: sistemas, bases de datos, formularios, expedientes, aplicaciones web, planillas, correos, papelería, dispositivos, registros y flujos interinstitucionales.

🔵 2. Clasifica cada activo según el tipo de PII que maneja

Define si contiene:

- Datos personales
- Datos sensibles
- Datos de niños, adolescentes, usuarios sociales, beneficiarios, funcionarios

  Esto determina criticidad y controles.

🔵 3. Incluye la finalidad y base legal asociada al activo

Cada activo debe responder a:

- ¿Para qué existe?
- ¿Cuál es la finalidad?
- ¿Cuál es la base legal del tratamiento?

  Sin esto → no hay cumplimiento de la Ley 21.719.

🔵 4. Registra el proceso institucional al que pertenece el activo

Asóciale:

- Unidad responsable
- Trámite o proceso misional
- Actividad de tratamiento donde participa

  Permite evidenciar trazabilidad y responsabilidades.

🔵 5. Documenta ubicación, custodios y responsables

Indica:

- Custodio técnico (TI)
- Responsable funcional (unidad misional)
- Encargado del tratamiento si aplica

  Esto asegura control operacional.

🔵 6. Registra flujos de datos internos y externos

Para cada activo documenta:

- Con quién comparte datos
- Qué datos se transfieren
- Medios de transporte (API, correo, plataforma, físico)

  Esto escanea riesgos de interoperabilidad estatal.

🔵 7. Incluye riesgos asociados al activo desde la perspectiva de privacidad

Ejemplos:

- Accesos no autorizados
- Exposición pública por transparencia
- Vulnerabilidades en sistemas legacy
- Brechas por proveedores

  Un inventario sin valoración de riesgo queda incompleto.

🔵 8. Mantén el inventario vivo, con control de cambios y revisión periódica

Debe actualizarse cuando:

- Cambia un sistema
- Se crea un nuevo trámite
- Se modifica una finalidad
- Se integra un proveedor

  Es un documento dinámico, no estático.

Contexto General de Riesgos

🔵 **1. Filtración de datos sensibles de beneficiarios**

Criticidad: Alto impacto social; pérdida de confianza ciudadana; riesgo político; exposición mediática inmediata.

🔵 **2. Publicación de actos administrativos con datos personales sin anonimizar**

Criticidad: Incumplimiento directo de la Ley 21.719; riesgo de sumarios; observaciones de Contraloría.

🔵 **3. Acceso no autorizado en sistemas legacy**

Criticidad: Sistemas antiguos sin trazabilidad → brechas silenciosas y difícil detección; alta probabilidad.

🔵 **4. Procesamiento de datos sin base legal o con finalidad difusa**

Criticidad: Vulneración del principio de licitud; sanciones ANPD; cuestionamiento público de legitimidad institucional.

🔵 **5. Interoperabilidad sin evaluación de finalidad o proporcionalidad**

Criticidad: Alto riesgo de uso indebido entre organismos; falta de trazabilidad; dependencia de terceros.

🔵 **6. Manejo inadecuado de datos en Atención Ciudadana**

Criticidad: Errores humanos, traspaso informal de datos, impresión innecesaria; alta frecuencia de incidentes.

🔵 **7. Retención excesiva de datos por normas administrativas antiguas**

Criticidad: Acumulación de PII obsoleta; mayor exposición en caso de incidente; impacto masivo.

🔵 **8. Falta de procedimientos ARCO+ claros y trazables**

Criticidad: Reclamos ciudadanos; incumplimiento directo de la ley; pérdida de legitimidad operativa.

🔵 **9. Proveedores externos sin controles adecuados de privacidad (Encargados)**

Criticidad: Alto riesgo por tercerización; incidentes que afectan al organismo pero sin control directo.

🔵 **10. Riesgos en teletrabajo o trabajo híbrido**

Criticidad: Accesos remotos inseguros; pérdida de documentos físicos; uso indebido de dispositivos personales.

🔵 **11. Incidentes de privacidad no detectados o no reportados a tiempo**

Criticidad: Sanciones por notificación tardía; aumento del impacto; incremento del daño reputacional.

🔵 **12. Ausencia de DPIA en programas sociales de alto impacto**

Criticidad: Tratamientos de alto riesgo sin análisis previo; exposición política y regulatoria; impacto impredecible.

🔵 **13. Brechas en correos electrónicos institucionales (phishing / fuga)**

Criticidad: Exfiltración rápida de información; vectores comunes de incidentes; impacto transversal.

🔵 **14. Acceso privilegiado mal gestionado en bases de datos**

Criticidad: Riesgo interno crítico; difícil trazabilidad; posibilidad de uso indebido o extracción silenciosa.

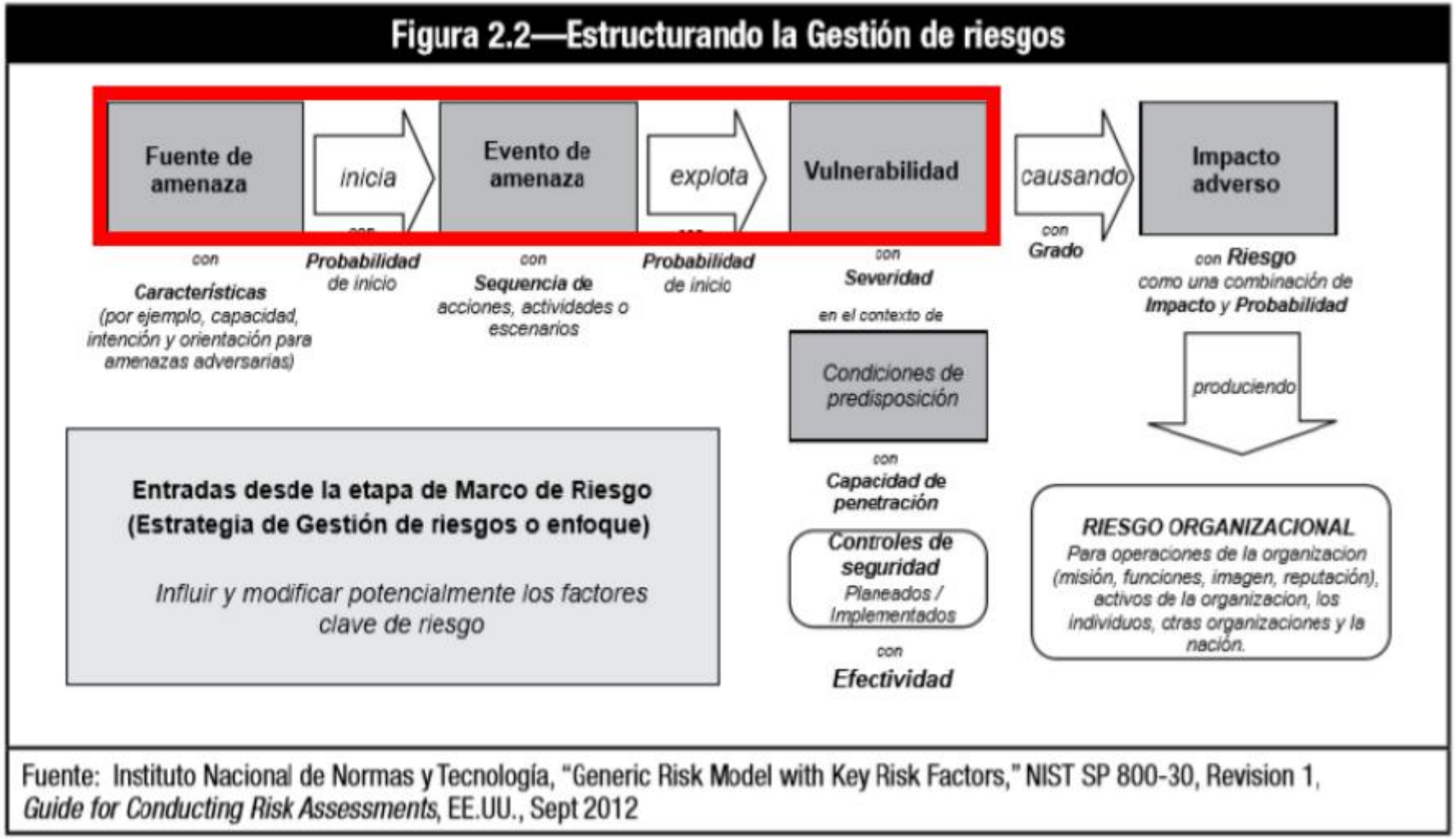
🔵 **15. Tratamiento masivo de datos sin controles de minimización**

Criticidad: Procesos que recolectan más información de la necesaria; alto riesgo de exposición.

🔵 **16. Integración con sistemas externos sin garantías técnicas ni legales**

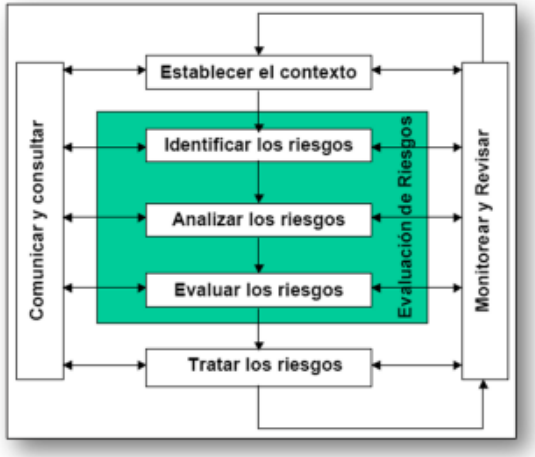
Criticidad: Flujos no documentados; dependencia tecnológica; vulneración de principios de transferencia y seguridad.

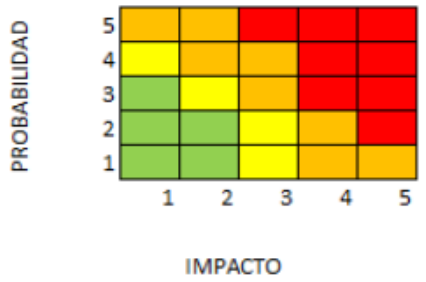
Riesgos de Ciberseguridad

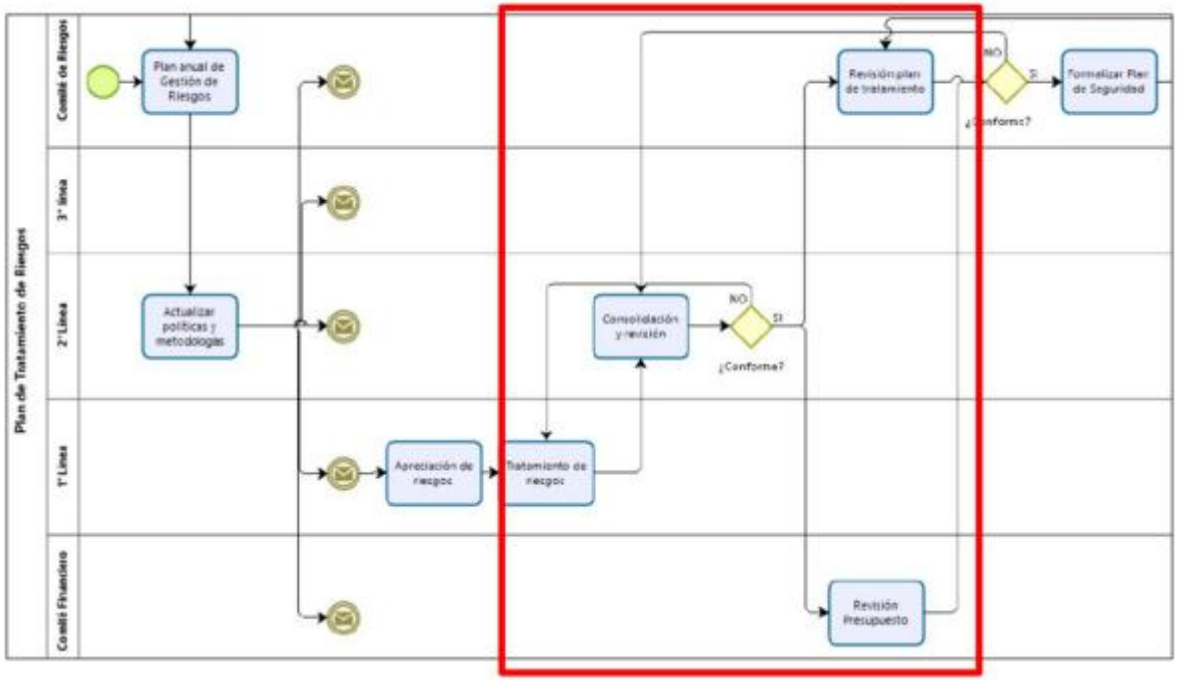


Fuente: Instituto Nacional de Normas y Tecnología, "Generic Risk Model with Key Risk Factors," NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*, EE.UU., Sept 2012

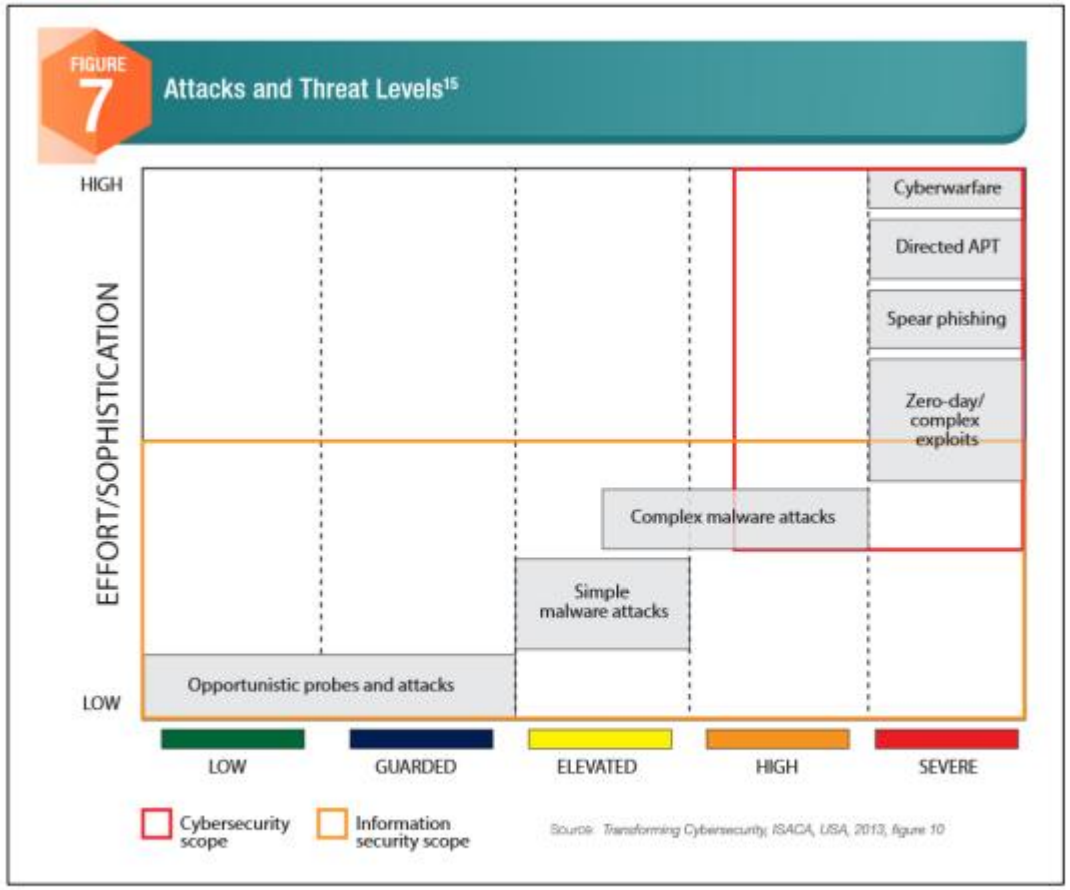
Riesgos de Ciberseguridad







Amenaza



Fuente: European CybersecurityImplementation: Overview, ISACA

enisa-threat-landscape-2023

Medidas de Protección

International Organization for Standardization
ISO
27002

CIS Controls
Version 8

01	Inventory and Control of Enterprise Assets
02	Inventory and Control of Software Assets
03	Data Protection
04	Secure Configuration of Enterprise Assets and
05	Account Management
06	Access Control Management
07	Continuous Vulnerability Management
08	Audit Log Management
09	Email and Web Browser Protections
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing

MITRE
ATT&CK™

Desafío crucial: Tener un Plan de Implementación

1.- Creación de la Urgencia

2.- Formar una coalición

3.- Comprender el Estado Actual

4.- Entender el Contexto

5.- Formulación de Objetivos

6.- Plan de Implementación

7.- Formalización de Comité de Seguridad de la Información

8.- Programa de capacitación, entrenamiento y concientización

9.- Definir la Gobernanza y Gestión de la Seguridad de la Información

10.- Establecimiento del Política de Seguridad

11.- Implementación de procedimientos de apoyo del SGSI

12.- Implementación de procedimientos y controles bases del SGSI

13.- Definir Metodología e Implementación de Apreciación de Riesgos

14.- Desarrollar el Plan de Tratamiento de Riesgos

15.- Implementación de Políticas, Procedimientos y Controles

16.- Gestión de Indicadores de Performance

17.- Monitoreo del SGSI

18.- Auditoría al SGSI

19.- Revisión de la Dirección al SGSI

20.- Mejora Continua

21.- Preparación para la Auditoría Certificación

Ver Presentación Linkedin

Clausula Soporte

Clausula	Requisito	Actividad requerida	Medios de Verificación
7.1	Recursos	La organización determina y proporciona los recursos para establecer, implementar, mantener y mejorar continuamente el SGSI.	- Plan de implementación - Presupuesto
7.2	Competencia	La organización determina la competencia de las personas necesarias para el desempeño de la seguridad de la información y asegura que las personas sean competentes.	- Perfiles de Cargo Claves - DNC (Detección de necesidades de capacitación) - Plan de capacitación - Plan de concienciación - Desarrollo de actividades de concienciación y capacitación
7.3	Concienciación	La organización informa a las personas sobre la política de seguridad de la información, su contribución a la eficacia del SGSI, los beneficios de mejorar la seguridad de la información y las implicaciones de no cumplir con los requisitos del SGSI.	
7.4	Comunicación	La organización determina las necesidades de comunicaciones internas y externas relacionadas con el SGSI.	- Proceso de Comunicaciones - Plan de Comunicaciones
7.5	Información documentada	La organización incluye información documentada en el SGSI según lo requiere directamente la norma ISO 27001, así como también lo determina la organización como necesaria para la eficacia del SGSI	- Proceso de Gestión Documental - Plantillas de Documentos - Maestro de Documentos

Se requiere un presupuesto especifico para las acciones de SGSI y SGIP

Clausula Soporte

Clausula	Requisito	Actividad requerida	Medios de Verificación
7.1	Recursos	La organización determina y proporciona los recursos para establecer, implementar, mantener y mejorar continuamente el SGSI.	- Plan de implementación - Presupuesto
7.2	Competencia	La organización determina la competencia de las personas necesarias para el desempeño de la seguridad de la información y asegura que las personas sean competentes.	- Perfiles de Cargo Claves - DNC (Detección de necesidades de capacitación) - Plan de capacitación - Plan de concienciación - Desarrollo de actividades de concienciación y capacitación
7.3	Concienciación	La organización informa a las personas sobre la política de seguridad de la información, su contribución a la eficacia del SGSI, los beneficios de mejorar la seguridad de la información y las implicaciones de no cumplir con los requisitos del SGSI	
7.4	Comunicación	La organización determina las necesidades de comunicaciones internas y externas relacionadas con el SGSI.	- Proceso de Comunicaciones - Plan de Comunicaciones
7.5	Información documentada	La organización incluye información documentada en el SGSI según lo requiere directamente la norma ISO 27001, así como también lo determina la organización como necesaria para la eficacia del SGSI	- Proceso de Gestión Documental - Plantillas de Documentos - Maestro de Documentos

Se requiere una formación diferenciada en roles y funciones!!

Clausula Soporte y Operación

Clausula	Requisito	Actividad requerida	Medios de Verificación
8.1	Planificación y control operacional	La organización planifica, implementa y controla los procesos, sus requisitos y documentación requerida, de forma interna como externa, para alcanzar sus objetivos y gestionar los riesgos de seguridad de la información.	- Plan de implementación - Plan de Tratamiento de Riesgos
8.2	Evaluación de los riesgos de seguridad de la información	La organización efectúa evaluaciones de riesgos de seguridad de la información a intervalos planificados, y cuando se propongan o se produzcan modificaciones importantes	- Proceso de Gestión de Riesgo - Matriz de Riesgos - Plan de Tratamiento de Riesgos
8.3	Tratamiento de los riesgos de seguridad de la información	La organización implementa el plan de tratamiento de los riesgos de seguridad de la información.	- Plan de implementación - Plan de Tratamiento de Riesgos

Implementación de Políticas, Procedimientos y Controles

Se implementan de diversa forma, con diversos mecanismos y recursos.

Establezca claramente los alcances de la implementación de controles, evalué la pertinencia de la documentación y el uso de recursos (persona, tecnologías, servicios, infraestructura, entre otros).

Clausulas Evaluación

Clausula	Requisito	Actividad requerida	Medios de Verificación
9.1	Seguimiento, medición, análisis y evaluación	La organización realiza el seguimiento, medición, análisis y evaluación del SGSI para determinar su desempeño y eficacia.	- Objetivos del SGSI - Mapa de KPI - Cuadro de Mando Integral - Plan de implementación
9.2	Auditoría interna	La organización realiza auditorías internas a intervalos planificados en los procesos y riesgos claves de la seguridad de la información	- Proceso de Auditoría - Plan de auditoría - Programas de auditoría - Informes de auditoría - Informes de seguimiento
9.3	Revisión por la dirección	La dirección realiza revisiones periódicas de los resultados de la gestión de seguridad de la información y tomas las acciones necesarias para la mejora continua.	- Plan de Revisión de Dirección - Plantilla de Presentación - Actas de Revisión

Auditoría Interna del SGSI + SGIP

Understand the Business	Define IT Universe	Perform Risk Assessment	Formalize Audit Plan
• Identify the organization's strategies & business objectives • Understand the high risk profile for the organization • Identify how the organization structures their business operations • Understand the IT service support model	• Dissect the business fundamentals • Identify significant applications that support the business operations • Identify critical infrastructure for the significant applications • Understand the role of supporting technologies • Identify major projects and initiatives • Determine realistic audit subjects	• Develop processes to identify risks • Assess risk and rank audit subjects using IT risk factors • Assess risk and rank subjects using business risk factors	• Select audit subjects and bundle into distinct audit engagements • Determine audit cycle and frequency • Add appropriate engagements based on management requests or opportunities for consulting • Validate the plan with business management

Las capacidades de los auditores es una importante brecha a subsanar, la actividad es el clave para el aseguramiento y mejora del SGSI, principalmente en la evaluación de controles y actividades criticas.

Gestión de Indicadores Claves

Deben medir una gestión que sea necesaria de controlar y pueda aportar en la mejora continua

Related ISMS processes and controls (Clause or control number in ISO/IEC 27001:2013)	Measurement construct example names
5.1, 7.1	B.2 Resource allocation
7.5.2, A.5.1.2	B.3 Policy review
5.1, 9.3	B.4 Management commitment
8.2, 8.3	B.5 Risk exposure
9.2, A.18.2.1	B.6 Audit programme
10	B.7 Improvement actions
10	B.8 Security incidents cost
10, A.16.1.6	B.9 Learning form information security incidents
10.1	B.10 Corrective action implementation
A.7.2	B.11 ISMS training or ISMS awareness
A.7.2.2	B.12 Information security training
A.7.2.1, A.7.2.2	B.13 Information security awareness compliance
A.7.2.2	B.14 ISMS awareness campaigns effectiveness
A.7.2.2, A.9.3.1, A.16.1	B.15 Social engineering preparedness
A.9.3.1	B.16 Password quality – manual
A.9.3.1	B.17 Password quality – automated
A.9.2.5	B.18 Review of user access rights
A.11.1.2	B.19 Physical entry controls system evaluation
A.11.1.2	B.20 Physical entry controls effectiveness
A.11.2.4	B.21 Management of periodic maintenance
A.12.1.2	B.22 Change management
A.12.2.1	B.23 Protection against malicious code
A.12.2.1	B.24 Anti-malware
A.12.2.1, A.17.2.1	B.25 Total availability
A.12.2.1, A.13.1.3	B.26 Firewall rules
A.12.4.1	B.27 Log files review
A.12.6.1	B.28 Device configuration
A.12.6.1, A.18.2.3	B.29 Pentest and vulnerability assessment
A.12.6.1	B.30 Vulnerability landscape
A.15.1.2	B.31.1/B.31.2 Security in third party agreements
A.16	B.32 Security incident management effectiveness
A.16.1	B.33 Security incidents trend
A 16.1.3	B.34 Security event reporting
A.18.2.1	B.35 ISMS review process
A.18.2.3	B.36 Vulnerability coverage

ISO 27004 –
Indicadores del SGSI

Defínalos a un alto nivel de actividades (son claves), a nivel de procesos es una buena práctica, cuestiónese la utilidad y su pertinencia de uso, principalmente en la toma de decisiones.

Revisión de la Dirección

La revisión de la dirección debe ser periódica e integral, recogiendo todos los puntos de atención necesarios que signifiquen una potencial de brecha en los objetivos establecidos o una desviación, tomando decisiones oportunas para su corrección o fortalecimiento de medidas.

Clausula Mejora

Clausula	Requisito	Actividad requerida	Medios de Verificación
10.1	Mejora continua	La organización establece un proceso para mejora la idoneidad, adecuación y eficacia del sistema de gestión de la seguridad de la información.	- Procesos de Mejora Continua - Plan de Implementación
10.2	No conformidad y acciones correctivas	La organización establece un proceso para gestionar de manera oportuna las no conformidad y oportunidades de mejoras, realizando los análisis de causas necesarios para su identificación	- Proceso de Gestión de no conformidades - Análisis de causas - Cierre de no conformidades

Próximas actividades

MARTES 06 DE ENERO – 11:00 A 13:00 HRS (GMT-3 Hora Chile)

MIÉRCOLES 07 DE ENERO – 11:00 A 13:00 HRS (GMT-3 Hora Chile)

JUEVES 08 DE ENERO – 11:00 A 13:00 HRS (GMT-3 Hora Chile)

VIERNES 09 DE ENERO – 11:00 A 13:00 HRS (GMT-3 Hora Chile)

https://alignment.cl/programa-de-cumplimiento-digital/

Próximas cursos Avanzados

CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

Componentes Claves SGSI + SGIP

Ciclo de Workshops

ALIGNMENT
SOLUCIONES ESTRATÉGICAS

DIPLOMADO
CIBERSEGURIDAD