CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

Ley Marco de Ciberseguridad 21633

Workshop N°1

ALIGNMENT
SOLUCIONES ESTRATÉGICAS

DIPLOMADO
CIBERSEGURIDAD

Agenda

- Conociendo la Ley Marco de Ciberseguridad – Ley 21633
- Institucionalidad y Gobernanza
- Servicios Esenciales y Operadores de Importancia Vital (OIV)
- Definiciones claves de la Ley
  - Sistema de Gestión de Seguridad de la Información (SGSI)
  - Continuidad operacional y ciberseguridad
  - Operaciones de revisión, ejercicios y simulacros
  - Reporte de Incidentes
  - Formación en Ciberseguridad: Perfiles de Ciberseguridad (ANCI)
- Desafíos de la Ley

ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD

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:

Profesor

Carlos Lobos de Medina

Ingeniero Civil en Informática y Magister en Informática © de la Universidad de Santiago de Chile, Diplomado en Auditoría de Sistemas, Postitulado en Seguridad Computacional 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.}

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

Conociendo la Ley Marco de Ciberseguridad – Ley 21633

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]

Institucionalidad y Gobernanza

Funciones de la Agencia Nacional de Ciberseguridad (ANCI)

1. Asesorar al Presidente de la República en la elaboración y aprobación de la Política Nacional de Ciberseguridad;
2. Aplicar e interpretar administrativamente las disposiciones legales y reglamentarias en materia de ciberseguridad;
3. Coordinar y supervisar al **CSIRT Nacional**;
4. Establecer una coordinación con el CSIRT de la **Defensa Nacional** en lo relativo a los estándares y tiempos de comunicación de incidentes de ciberseguridad o vulnerabilidades, y respecto a las materias que serán objeto de intercambio de información;
5. Calificar a los servicios esenciales y operadores de importancia vital;
6. Diseñar e implementar planes y acciones de formación ciudadana, capacitación, fortalecimiento, difusión y promoción de la cultura en ciberseguridad;
7. Cooperar con organismos públicos e instituciones privadas, en materias propias de su competencia, sin perjuicio de las atribuciones de otros organismos del Estado;

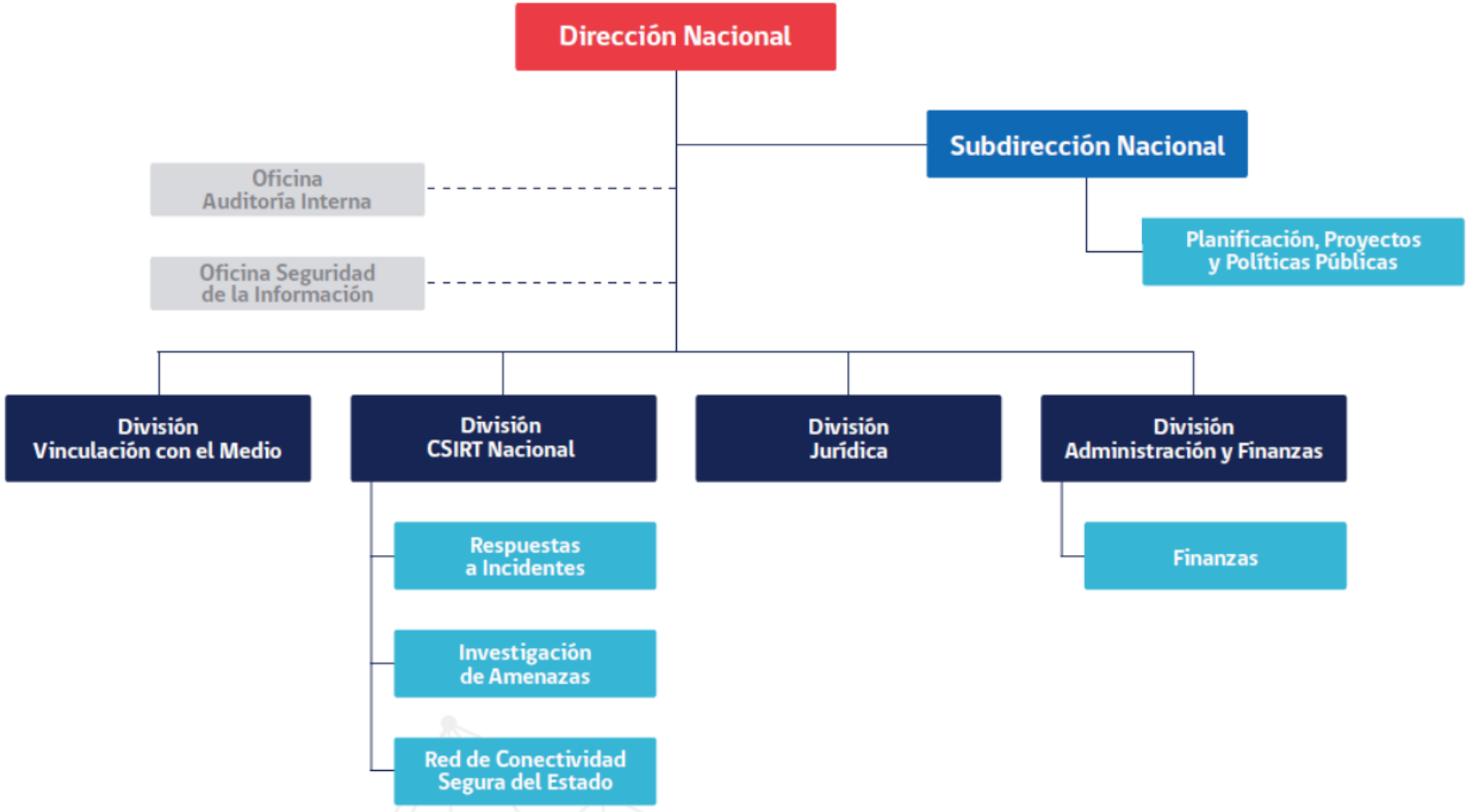
Fuente: https://anci.gob.cl/quienes-somos/mision-y-objetivos/

Funciones de la Agencia Nacional de Ciberseguridad (ANCI)

8. Otorgar y revocar las acreditaciones correspondientes a los centros de certificación, en los casos y bajo las condiciones que establezca esta ley y el reglamento respectivo;
9. Fomentar la investigación, innovación, capacitación y entrenamiento frente a amenazas, vulnerabilidades e incidentes de ciberseguridad
10. Certificar el cumplimiento de los estándares de ciberseguridad correspondientes por parte de los organismos de la Administración del Estado;
11. Establecer los estándares que deberán cumplir las instituciones que provean bienes o servicios al Estado, y las normas de seguridad para el desarrollo de los sistemas y programas informáticos que serán utilizados por los organismos del Estado;
12. Establecer estándares de ciberseguridad y deberes de información al público sobre riesgos de ciberseguridad de dispositivos digitales disponibles a consumidores finales;
13. Administrar la Red de Conectividad Segura del Estado.

Fuente: https://anci.gob.cl/quienes-somos/mision-y-objetivos/

Estructura de la ANCI



CSIRT Nacional y CSIRT Sectoriales

Funciones del CSIRT Nacional

De acuerdo al detalle del artículo 24, las funciones de este Equipo son:

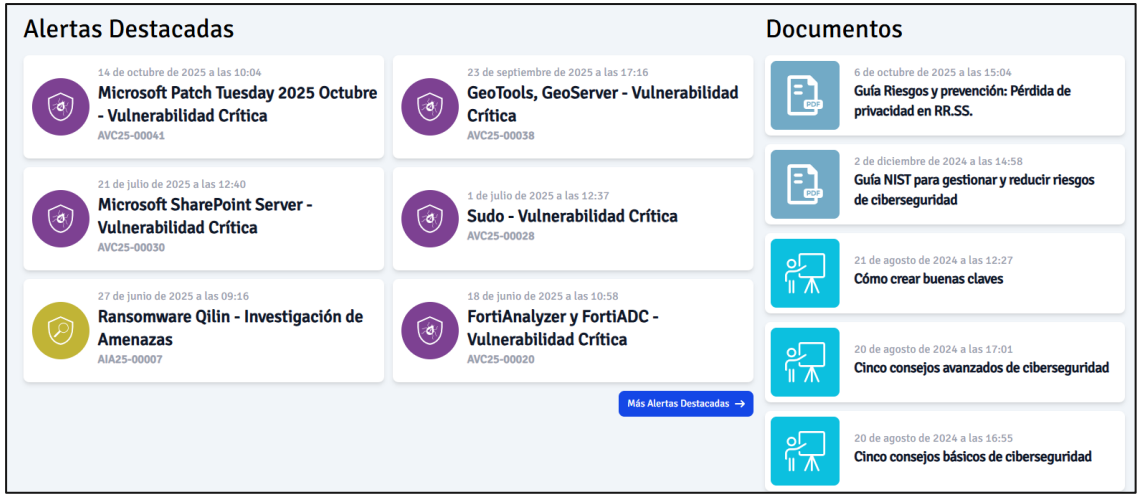
1. **Responder ante ciberataques o incidentes de ciberseguridad**, cuando éstos sean de efecto significativo.
2. **Coordinar a los CSIRT que pertenezcan a organismos de la Administración del Estado** frente a ciberataques o incidentes de ciberseguridad de efecto significativo. Esta coordinación deberá establecerse también con el CSIRT de la Defensa Nacional.
3. **Servir de punto de enlace** con CSIRT extranjeros.
4. **Prestar colaboración o asesoría técnica a los CSIRT de organismos de la Administración del Estado** en la implementación de políticas y acciones sobre ciberseguridad.
5. **Supervisar incidentes a escala nacional**.

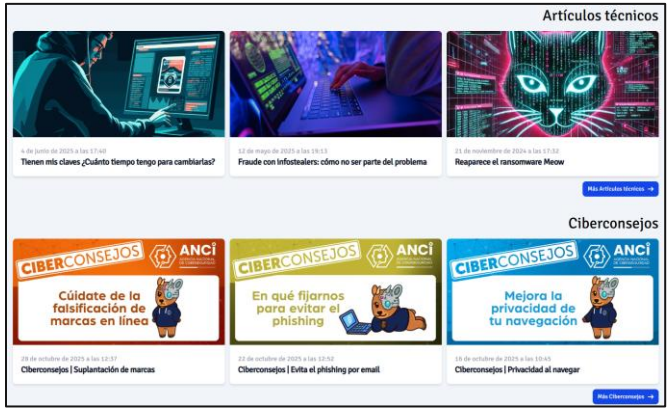
Sobre riesgos, incidentes y vulnerabilidades, el CSIRT Nacional debe:

1. **Efectuar un análisis dinámico de riesgos e incidentes** y de conocimiento de la situación.
2. **Requerir a las instituciones afectadas** o a los CSIRT correspondientes **información anonimizada de incidentes de ciberseguridad y vulnerabilidades** encontradas y los planes de acción respectivos para mitigarlos.
3. **Difundir alertas tempranas**, avisos e información sobre riesgos e incidentes para la comunidad.

Adicionalmente, CSIRT Nacional debe:

1. **Realizar entrenamiento, educación y capacitación** en materia de ciberseguridad.
2. **Elaborar un informe con los criterios** técnicos para determinar las categorías **qué tipos de incidentes o vulnerabilidades estarán eximidas de notificación**.





Estructura y Funcionamiento de los CSIRT - OEA

Otras definiciones orgánicas relevantes

- Comité Interministerial de Ciberseguridad

- Ministerio del Interior y Seguridad Pública
- Ministerio de Relaciones Exteriores
- Ministerio de Defensa Nacional
- Ministerio de la Secretaría General de la Presidencia
- Ministerio de Hacienda
- Ministerio de Economía, Fomento y Turismo
- Ministerio de Ciencia, Tecnología, Conocimiento e Innovación
- Agencia Nacional de Inteligencia (ANI)

- Comité Multisectorial de Ciberseguridad

- El director o directora nacional de la ANCI.
- Representantes del sector industrial o comercial.
- Representantes del mundo académico.
- Representantes de organizaciones de la sociedad civil

Servicios Esenciales y Operadores de Importancia Vital (OIV)

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?

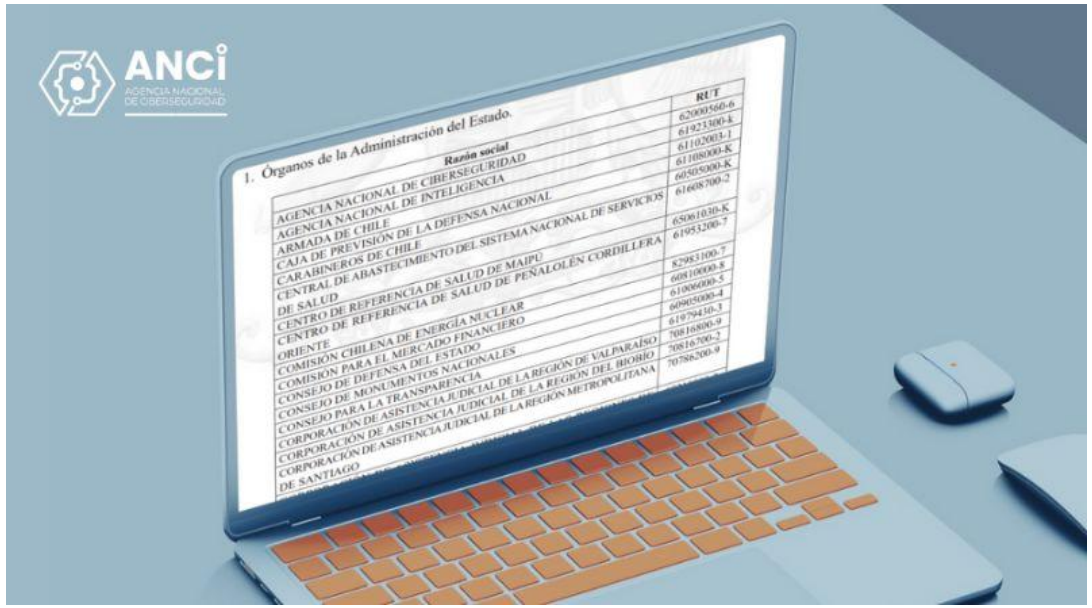
...por **instituciones privadas** que realicen las siguientes actividades:

- 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)

Definiciones claves de la Ley

Definiciones de la Ley

- **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

Promulgación de la Ley

"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 que protegerlos?

- Amenazas
- Vulnerabilidades

¿Cómo protegerlos?

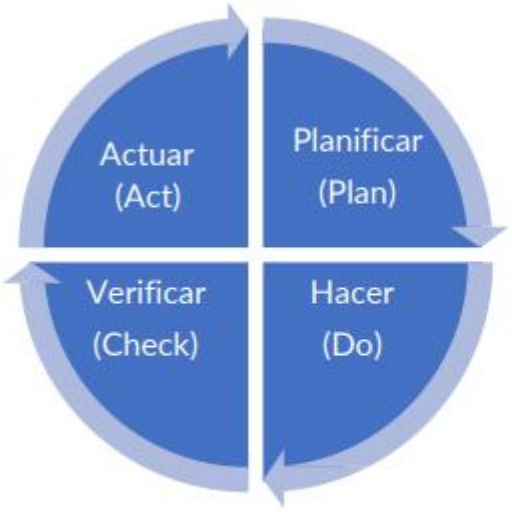
- Con una metodología
- Con prácticas de gestión de riesgo
- Implementando controles
- Con un proceso estructurado
- Mejorando continuamente

Fuente: Managing Information Security Risk – Christopher Albert.2003

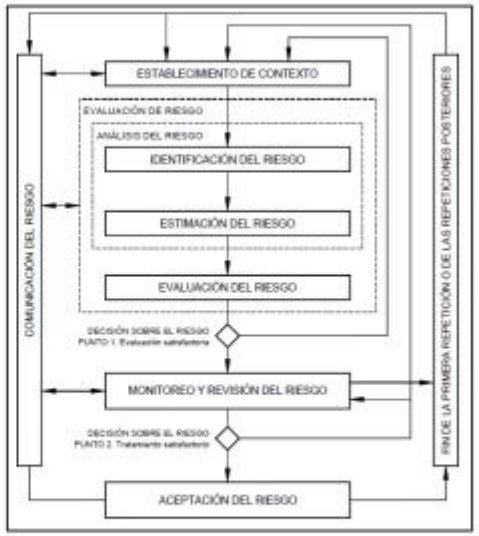
¿Que Ofrece ISO 27001?

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

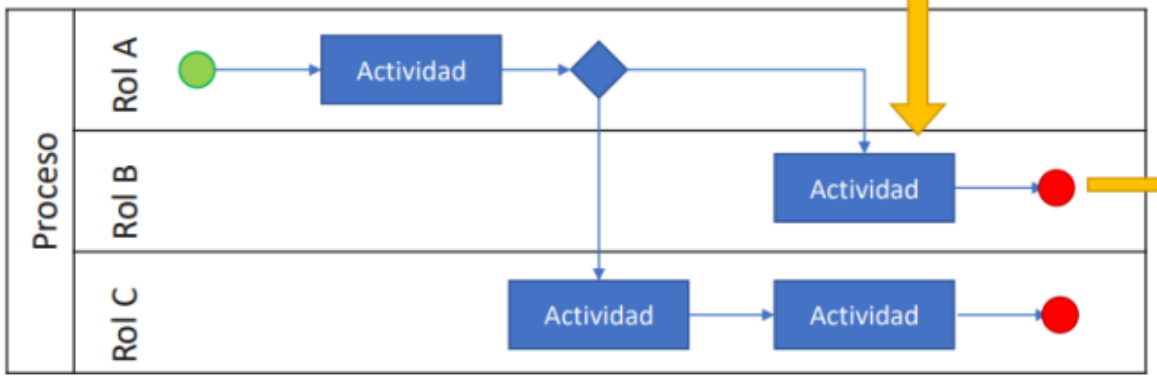
Describe como el proceso se lleva a cabo

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

Ecosistema de Normas

ISO 27.003
Directrices de Implementación

ISO 27.004
Indicadores del SGSI

ISO 27.022
Procesos del SGSI

ISO 27014
Gobierno de la Ciberseguridad

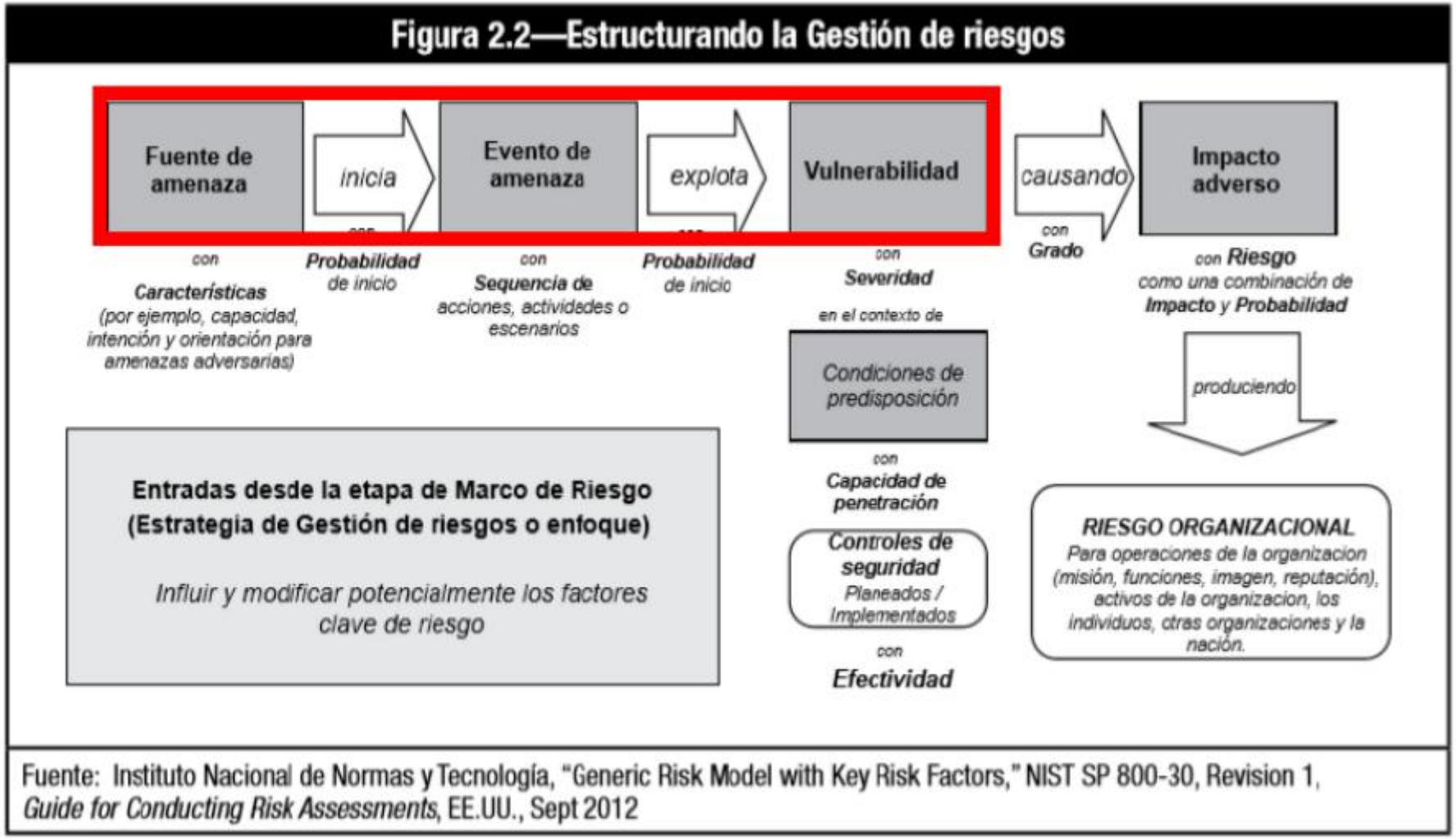
ISO 27701
Gestión de la Privacidad

ISO 27033
Seguridad en Redes

ISO 27034
Seguridad en Aplicaciones

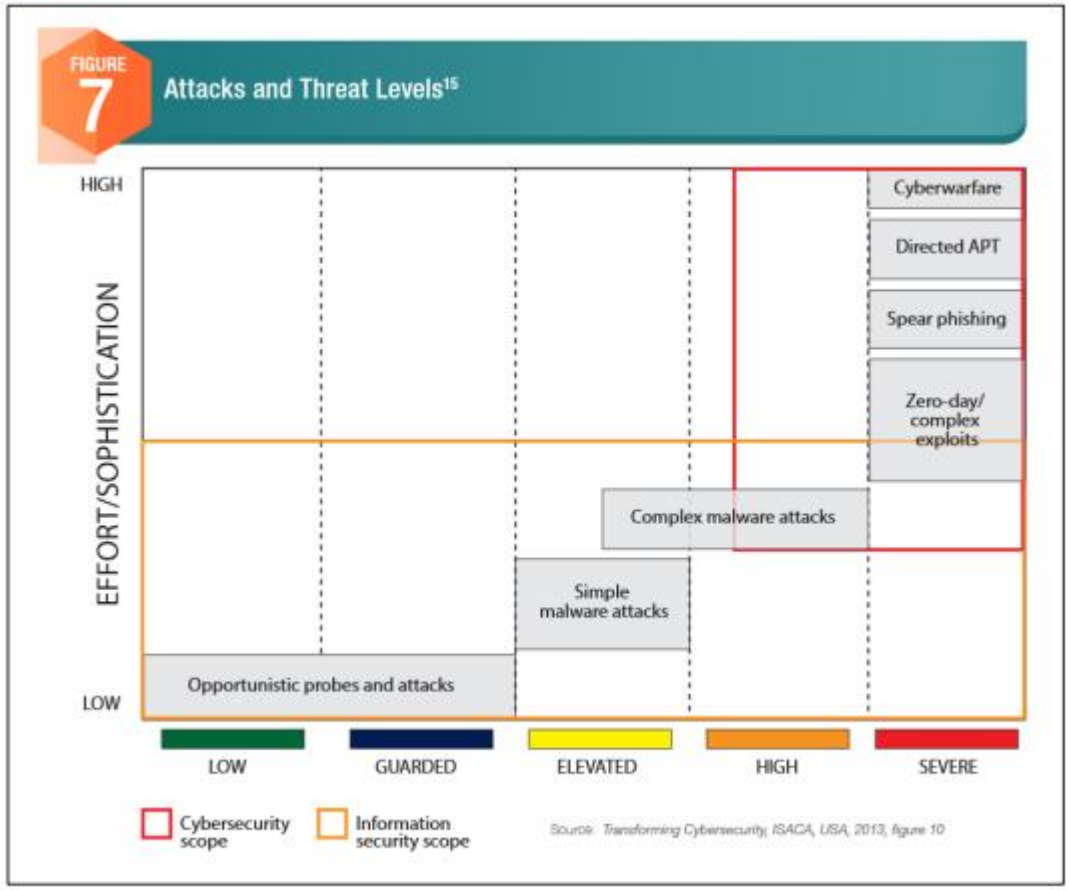
ISO 27037
Evidencia Electrónica

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

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™

Que controles son cruciales y operaciones?

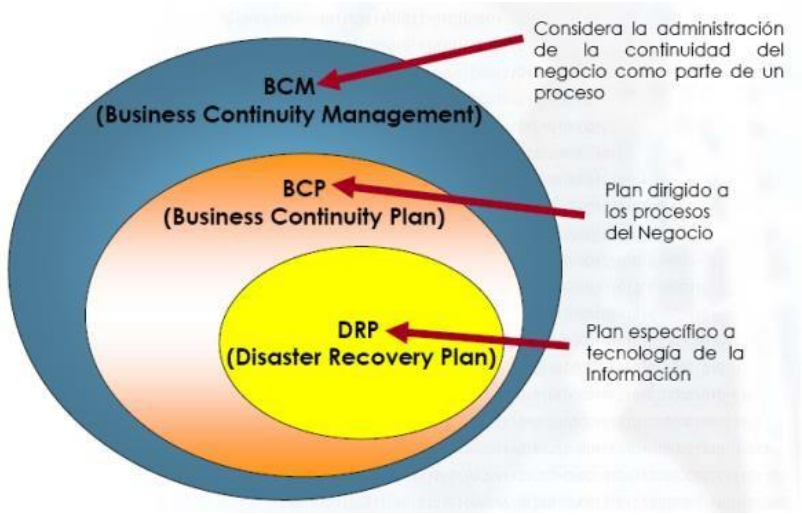
REQUISITO DE LA LEY

Elaborar e implementar planes de continuidad operacional y ciberseguridad.

REQUISITO DE LA LEY

Adoptar de forma oportuna medidas para reducir el impacto y la propagación de un incidente de ciberseguridad.

Evolución de la Continuidad del Negocio



DRP

Disaster Recovery Plan

- Plan orientado principalmente a recuperar todo lo relacionado con TI
- Su enfoque típicamente es:
  - Los Datos
  - Los Servicios
  - Las Aplicaciones
  - El Sistema Operativo
- Con frecuencia se ve simplemente como un SITE Alterno

BCP

Business Continuity Plan

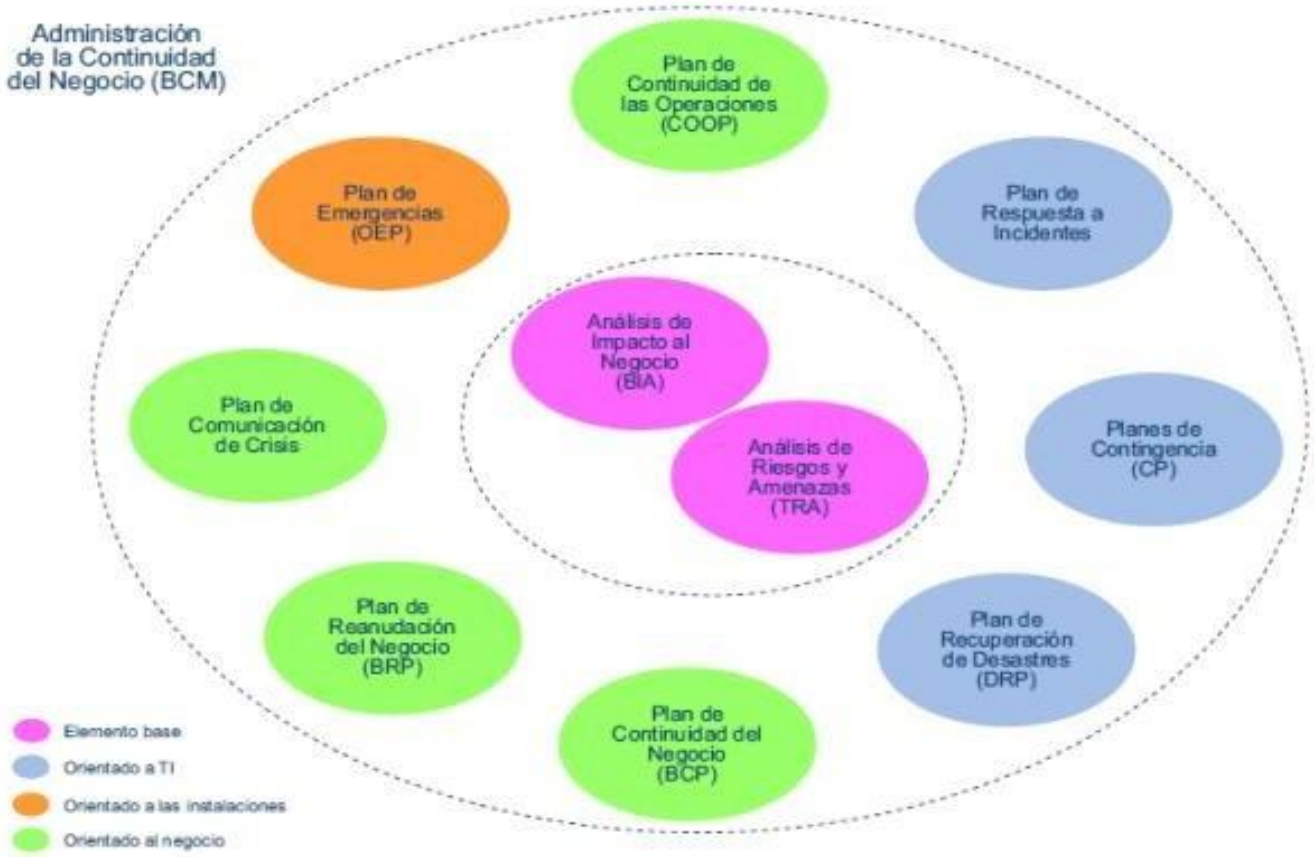
- Plan orientado a recuperar todas las funciones críticas de la empresa y que el negocio pueda operar
- Típicamente contiene
  - DRP
  - Comités
  - Plan de Emergencia
  - Notificaciones
  - Sitios alternos de trabajo

BCM

Busines Continuity Management

- Programa continuo para todas las funciones de la empresa orientado a que
  - Cultura de BC
  - Concientización
  - Actualizacíon de todos los cambios
  - Enfoque fuerte a probar el plan para irlo mejorando

Modelo del BCI y NIST



¿A que tipo de Incidentes estará expuesto?

CRÍTICO	Otros	APT
		Ciberterrorismo
		Daños informáticos PIC
MUY ALTO	Código dañino	Distribución de malware
		Configuración de malware
	Intento de intrusión	Ataque desconocido
	Intrusión	Robo
	Disponibilidad	Sabotaje
		Interrupciones
ALTO	Contenido abusivo	Pornografía infantil, contenido sexual o violento inadecuado
	Código dañino	Sistema infectado
		Servidor C&C (Mando y Control)
		Malware dominio DGA
	Intento de intrusión	Compromiso de aplicaciones
	Disponibilidad	DoS (Denegación de servicio)
		DDoS (Denegación distribuida de servicio)
	Compromiso de la información	Acceso no autorizado a información
		Modificación no autorizada de información

		Pérdida de datos
	Fraude	Phishing
MEDIO	Contenido abusivo	Discurso de odio
	Obtención de información	Ingeniería social
		Explotación de vulnerabilidades conocidas
	Intento de intrusión	Intento de acceso con vulneración de credenciales
	Intrusión	Compromiso de cuentas con privilegios
	Fraude	Uso no autorizado de recursos
		Derechos de autor
		Suplantación
	Vulnerable	Criptografía débil
		Amplificador DDoS
		Servicios con acceso potencial no deseado
		Revelación de información
		Sistema vulnerable
BAJO	Contenido abusivo	Spam
	Obtención de información	Escaneo de redes (scanning)
		Análisis de paquetes (sniffing)
	Intrusión	Compromiso de cuenta sin privilegios
	Otros	Otros

5.24 Planificación y preparación

Roles y Responsabilidades

- Método común de reporte
- Proceso de Gestión de Incidentes
- Proceso de Respuesta a Incidentes
- Competencia Profesional
- Identificar training requerido

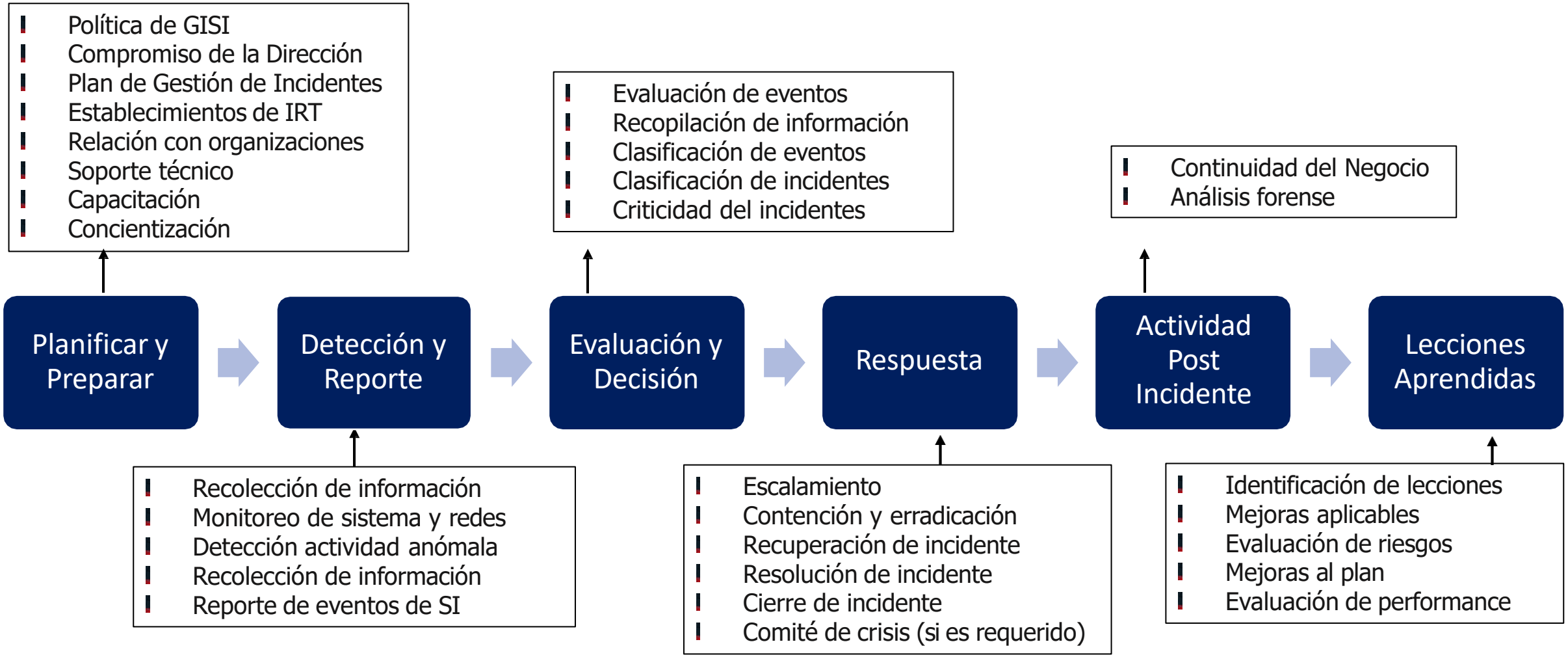
Procedimientos

- Evaluación de Eventos
- Detección y análisis de eventos e incidentes
- Escalamiento y Respuesta
- Manejo de Evidencia
- Análisis de la causa
- Lecciones Aprendidas

Procedimiento de Reporte

- Acciones frente a un evento
- Uso de Formularios
- Proceso de retroalimentación
- Creación de informes de incidentes

ISO 27.035-1 – Proceso de Gestión de Incidentes



Consideraciones bases

- Decreto Supremo 295 (2024) establece contenido y tiempos en los cuales los deben enviarse los reportes.

- Resolución 7 Exenta (2025) define la taxonomía de incidentes a reportar, es decir, que tipo de incidentes son los que deben ser reportados.

- Ley Marco (Articulo N°9) establece la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos en los términos del artículo 27° de la ley, tan pronto les sea posible y conforme al esquema establecido en dicho artículo.

- Debe poseerse los procedimientos y capacidades necesarias para dar respuesta a la Ley, sobre todo en los tiempos que esta define.

- Quienes deben reportar?
  - PSE y OIV

Consideraciones bases

Enviar una alerta temprana sobre la ocurrencia del evento en máximo 3 horas.

Actualización de la información con: evaluación inicial, gravedad, impacto e IoC, en 72 horas.

Informe final, máximo en 15 días corridos.

CSIRT Nacional podrá pedir actualizaciones.

OIV deberán informar al CSIRT Nacional plan de acción.

Los contratos no podrán contener ninguna cláusula que restringa o dificulte la comunicación de información sobre amenazas por parte del prestador de servicios.

La Agencia dictará instrucciones para la realización y recepción de los reportes.

Charla ANCI Ley Marco de Ciberseguridad 2025 marzo

Plan de Formación

ENISA – Roles de Ciberseguridad

NUEVO Diplomado en Arquitectura, Seguridad y DevSecOps en Azure

Programa Ejecutivo como Delegado de Protección de Datos

Diplomado en Arquitectura y Seguridad Cloud

Diplomado en Auditoría a la Ciberseguridad

Diplomado en Blue Team

Diplomado en Ciberseguridad Industrial

Diplomado en DevSecOps

Diplomado en Gobernanza, Gestión y Auditoría a la Ciberseguridad

Diplomado en Herramientas de Ciberseguridad

Diplomado en Implementación de Sistemas de Gobierno y Gestión de Ciberseguridad

Diplomado en Implementación de Privacidad y Cumplimiento

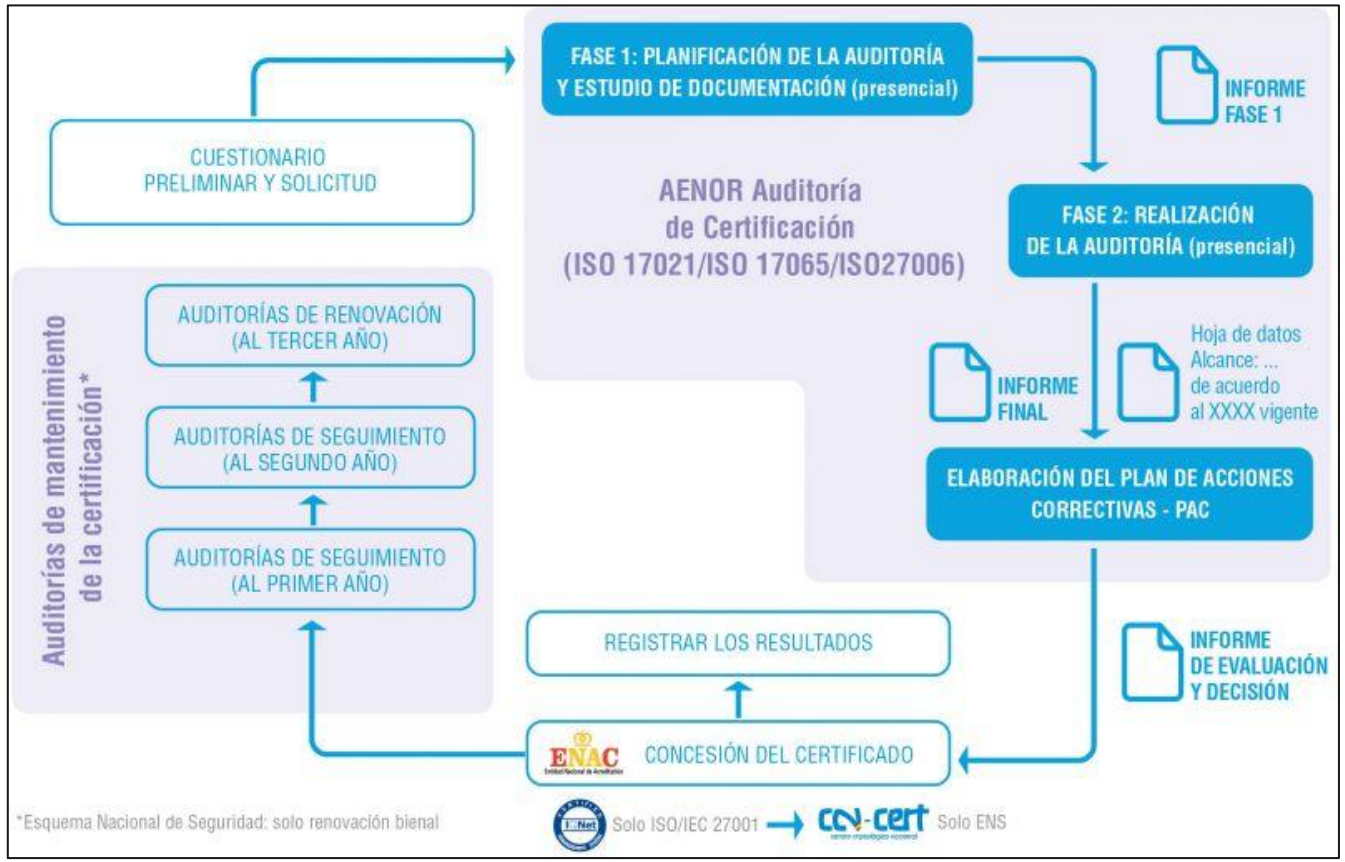
Diplomado en Red Team

Diplomado en Seguridad en Redes

Perfiles de la ANCI

1. **Jefe/a de Ciberseguridad:** Lidera la estrategia corporativa, define políticas y marcos de ciberseguridad, gestiona riesgos y asegura cumplimiento normativo (Ley Marco, ISO 27001, NIST, etc.).
2. **Operador(a) en Soporte de Ciberseguridad:** Ejecuta tareas de soporte técnico, gestión de incidentes y mantenimiento de controles operativos en infraestructura y redes.
3. **Controller de Ciberseguridad de Sistemas y Productos:** Supervisa la seguridad durante el ciclo de vida de productos y servicios tecnológicos, asegurando cumplimiento de políticas y estándares.
4. **Encargado(a) de Gestión de Riesgos Operativos y Continuidad Institucional:** Evalúa y mitiga riesgos tecnológicos y de continuidad del negocio, aplicando metodologías ISO 22301 e ISO 27005.
5. **Encargado(a) de Formación Técnica Profesional en Ciberseguridad:** Articula la formación técnica con las necesidades del sector, evaluando pertinencia curricular y empleabilidad.
6. **Encargado(a) de Hacking Ético:** Evalúa vulnerabilidades mediante pruebas de penetración y simulaciones controladas de ataque, conforme a principios éticos y estándares internacionales.
7. **Auditor(a) de Ciberseguridad:** Realiza auditorías técnicas y de cumplimiento, evalúa controles, conformidad y reporta hallazgos a la dirección.
8. **Analista de Ciberseguridad:** Monitorea eventos e incidentes en tiempo real, coordina la respuesta operativa y aplica protocolos de seguridad organizacional.
9. **Especialista en Seguridad en la Nube:** Implementa y gestiona controles de ciberseguridad en entornos cloud, protegiendo datos y asegurando continuidad operativa.
10. **Especialista en Operaciones de Ciberinteligencia:** Detecta, analiza y previene amenazas digitales mediante técnicas avanzadas de ciberinteligencia y análisis de comportamiento.

Proceso de Certificación



Desafíos de la Ley

Comprender las Infracciones asociadas (ART 39)

Infracciones Leves

1. No mantener el registro de las acciones de seguridad que señala la letra b).

2. No comunicar al CSIRT Nacional la realización continua de operaciones de revisión, ejercicios y demás acciones que señala la letra d).

3. No contar con programas de capacitación, formación y educación continua para los trabajadores, según dispone la letra h).

4. No designar un delegado de ciberseguridad, según dispone la letra i).

5. No dar cumplimiento a la instrucción particular de la Agencia en orden a certificar los planes de continuidad operacional del párrafo segundo de la letra c).

6. No contar con las certificaciones que exija la ley, de acuerdo con la letra f).

Infracciones Graves

1. No haber implementado el sistema de gestión de seguridad de la información continuo al que se refiere la letra a).

2. No haber elaborado o implementado los planes de continuidad operacional y ciberseguridad a los que se refiere la letra c).

3. No informar a los potenciales afectados sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente su información o redes y sistemas informáticos, en los casos que señala la letra g).

4. No adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad o un ciberataque, según señala la letra e).

5. La reincidencia en una misma infracción leve dentro del período de un año.

Infracciones Gravísimas

1. No adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad o un ciberataque, según señala la letra e), cuando éste posea un impacto significativo.

2. La reincidencia en una misma infracción grave dentro del período de un año.

Comprender las sanciones asociadas (ART 40)

Artículo 40. De las sanciones. La infracción a los preceptos de esta ley conlleva la imposición de una multa a beneficio fiscal, de acuerdo con la siguiente escala:

1. Las infracciones leves serán sancionadas con multa de hasta 5.000 unidades tributarias mensuales, o hasta 10.000 unidades tributarias mensuales si se trata de un operador de importancia vital.

2. Las infracciones graves serán sancionadas con multa de hasta 10.000 unidades tributarias mensuales, o hasta 20.000 unidades tributarias mensuales si se trata de un operador de importancia vital.

3. Las infracciones gravísimas serán sancionadas con multa de hasta 20.000 unidades tributarias mensuales, o hasta 40.000 unidades tributarias mensuales si se trata de un operador de importancia vital.

Implementación de un SGSI Desafío Clave

La comprensión de los procesos, controles y actividades claves de un SGSI resultan cruciales para la adopción de la Ley

[Workshops 2025 • Diplomados en Ciberseguridad]

La Integración con la Protección de Datos

La protección de datos, el gobierno de datos y la inteligencia artificial son nuevos desafíos criticos

[Workshops 2025 • Diplomados en Ciberseguridad]

Comprender los plazos y tiempos

- Se dispone de un año para la entrada en vigencia de la Ley (Abril 2026)
- ¿Que falta por definir?
  - Reglamentos específicos de operación
    - Definiciones propias del SGSI (ISO 27001/NIST CSF/Otro)
    - Gestión de Riesgos
    - Procedimientos operativos y controles
    - Planes de formación
  - Reglamentos de certificación
    - Organismos certificadores
    - Alcance
    - Características

Desafío crucial: Tener un Plan de Implementación

Ver Presentación Linkedin

CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

Ley Marco de Ciberseguridad 21633

Workshop N°1

ALIGNMENT
SOLUCIONES ESTRATÉGICAS

DIPLOMADO
CIBERSEGURIDAD