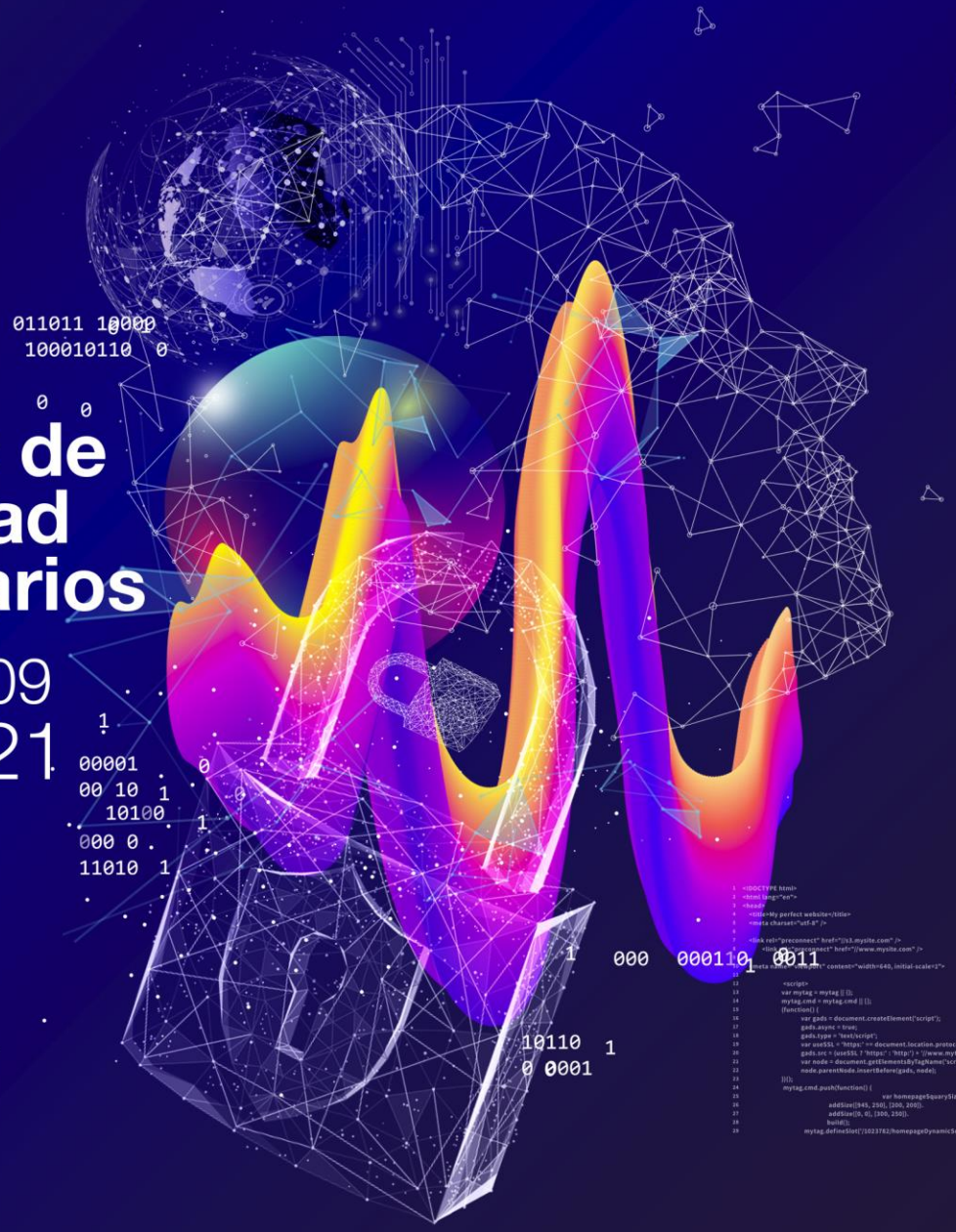
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos

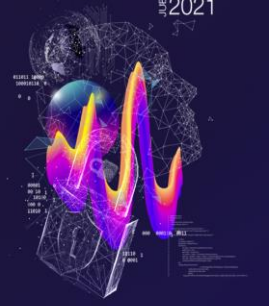
MARTES 28/09 2021



Políticas, procedimientos y controles para mitigar amenazas en ciberseguridad (SGSI)

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

2do Seminario de Ciberseguridad para funcionarios públicos JUEVES 28/09 2021



¿Cómo podemos mejorar la seguridad de la información?

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

"Contar con regulaciones adecuadas y conocidas, permitirá reducir los riesgos de seguridad."

ESTRATEGIA DEFINIDA

ISO 27001

- ✓ Utilizar estándares de seguridad ISO 27001
- ✓ Seleccionar controles de seguridad iniciales (30).
- ✓ Desarrollar e implementar Políticas y Procedimientos que soporten los controles seleccionados

OBJETIVO

Implementar un SGSI que permita:

- Fortalecer la Seguridad de la Información
- Mejorar nivel de madurez tecnológico de la organización

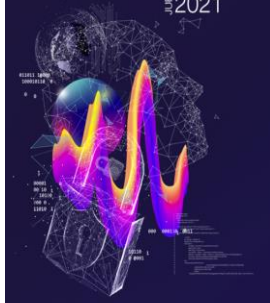
CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Estructura Normativa ISO 27001 - 27002

2do Seminario de Ciberseguridad para funcionarios públicos JUEVES 28/09 2021



Estructura Norma ISO 27001 - ISO 27002

DOMINIOS → **CONTROLES** → **POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN** | **POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN** | **PROCEDIMIENTOS ESPECÍFICOS DE SEGURIDAD DE LA INFORMACIÓN**

Dominios Norma ISO 27001

A.5 Políticas de Seguridad de la Información
A.6 Organización de la seguridad de la información
A.7 Seguridad ligada a los recursos humanos
A.8 Administración de activos
A.9 Control de acceso
A.10 Criptografía
A.11 Seguridad física y del ambiente
A.12 Seguridad de las operaciones
A.13 Seguridad de las comunicaciones
A.14 Adquisición, desarrollo y mantenimiento del sistema
A.15 Relaciones con el proveedor
A.16 Gestión de incidentes de seguridad de la información
A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio
A.18 Cumplimiento

Total Controles Norma ISO 27002

114 Controles asociados a los dominios mencionados.

Controles Seleccionados ISO 27002

A.05.01.01 Políticas para la seguridad de la información
A.06.01.01 Roles y responsabilidades de la seguridad de la información
A.07.02.02 Concientización, educación en seguridad de la información
A.08.01.01 Inventario de activos
A.09.01.01 Política de control del acceso
A.09.04.03 Sistema de gestión de contraseñas
A.11.01.01 Perímetro de seguridad física
A.12.01.04 Segregación de los ambientes (Desa., Test, Prod.)
A.12.02.01 Controles contra códigos maliciosos
A.12.03.01 Respaldo de la información
A.12.04.01 Registro de eventos
A.12.05.01 Instalación del software en sistemas operacionales
A.12.06.01 Gestión de las vulnerabilidades técnicas
A.13.01.01 Controles de Red
A.14.02.01 Política de desarrollo seguro
A.14.02.09 Prueba de aprobación del sistema
A.15.02.01 Supervisión y revisión de los servicios del proveedor
A.16.01.02 Informe de eventos de seguridad de la información
A.16.01.05 Respuesta ante incidentes de seguridad de la información
A.17.01.01 Planificación de la continuidad de la seguridad de la info.
A.18.02.03 Verificación del cumplimiento técnico

Política General, cubre aspectos transversales de la norma y establece la existencia de ésta en la Organización.

Políticas específicas que cubren los controles seleccionados

- De la organización de la seguridad de la información
- De administración de activos de información
- De seguridad física y del ambiente
- De gestión de comunicaciones y operaciones
- De control de acceso
- De gestión de incidentes de seguridad de la información
- De planificación de la continuidad de la seguridad de la Infor.
- De trabajo a distancia o teletrabajo.

Procedimientos específicos que cubren los controles seleccionados

- De Respaldo y Recuperación de La Información
- De Prevención de Programa Malicioso Informático
- De Gestión de identidad
- De Seguridad Física
- De Tercerización de Servicios TI
- Uso Correcto de Estaciones de Trabajo
- Uso Correcto de Servidores y Redes
- De Gestión de Incidentes

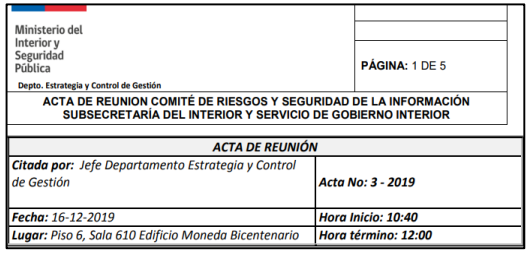
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Dominio (5) → Política de la seguridad de la información

Política General (PG-SGSI-001), cuyo principal objetivo es:

- Establecer los principios y marco general de trabajo para administrar, mantener, sensibilizar, monitorear y revisar el Sistema de Gestión de Seguridad de la Información (SGSI) acorde a las definiciones estratégicas y objetivos trazados por la Organización.

CONTROL	DESCRIPCIÓN	ORIENTACION SOBRE LA IMPLEMENTACION
A.05.01.01	Políticas para la seguridad de la información	En el nivel más alto, las organizaciones deberían definir una “política de seguridad de la información" que la aprueba la dirección y que establece el enfoque de la organización para administrar sus objetivos de seguridad de la información.
A.05.01.02	Revisión de las Políticas de Seguridad de la Información	Cada política debería tener un titular que tenga responsabilidad administrativa aprobada para el desarrollo, la revisión y la evaluación de ellas.


Ministerio del Interior y Seguridad Pública
Depto. Estrategia y Control de Gestión
PÁGINA: 1 DE 5
ACTA DE REUNION COMITÉ DE RIESGOS Y SEGURIDAD DE LA INFORMACIÓN
SUBSECRETARÍA DEL INTERIOR Y SERVICIO DE GOBIERNO INTERIOR
ACTA DE REUNIÓN
Citada por: Jefe Departamento Estrategia y Control de Gestión
Acta No: 3 - 2019
Fecha: 16-12-2019
Hora Inicio: 10:40
Lugar: Piso 6, Sala 610 Edificio Moneda Bicentenario
Hora término: 12:00

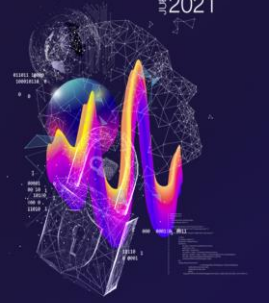

SUBSECRETARIA DEL INTERIOR
DIVISION JURIDICA
MINISTERIO DEL INTERIOR Y SEGURIDAD PUBLICA
27 DIC. 2011
OFICINA DE PARTES TOTALMENTE TRAMITADO
Sustituye disposiciones que indica de la Resolución Exenta N° 996, de 14 de marzo de 2005, de la Subsecretaría del Interior, sobre designación de Encargado de Seguridad de la Información del Ministerio del Interior y Seguridad Pública.
RESOLUCIÓN EXENTA N° 11.126
SANTIAGO, 26 DE DICIEMBRE DE 2011
HOY SE RESOLVIO LO QUE SIGUE
VISTO: Lo dispuesto en la Ley N° 20.502, que


Ministerio del Interior y Seguridad Pública
MINISTERIO DEL INTERIOR Y SEGURIDAD PUBLICA
08 MAR 2018
OFICINA DE PARTES TOTALMENTE TRAMITADO
APRUEBA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACION, DE LA SUBSECRETARIA DEL INTERIOR Y DEL SERVICIO DE GOBIERNO INTERIOR.
RESOLUCIÓN EXENTA N° 555
SANTIAGO, 23 DE ENERO DE 2018
VISTOS: Lo dispuesto en el D.F.L. N° 1/19653, de

Importancia:
Permite conocer el marco general de operación y alcance del SGSI de acuerdo con las definiciones estratégicas de la organización.

Dominio (6) → Organización de la seguridad de la información

2do Seminario de Ciberseguridad para funcionarios públicos JUEVES 28/09 2021



Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Política de organización de la seguridad de la información (PE-SGSI-001), +

Política de trabajo a distancia o teletrabajo (PE-SGSI-011), cuyos principales objetivos son:

- Establecer un marco de trabajo para la administración y directivos que permita controlar el funcionamiento de la seguridad de la información dentro de la organización.
- Asignar las responsabilidades en relación con seguridad de la información.
- Promover la segregación de funciones y definir Matriz de Responsabilidades de la Organización
- Definir las condiciones y las restricciones del uso del trabajo a distancia y del teletrabajo.

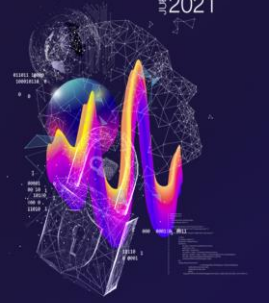
CONTROL	DESCRIPCIÓN	ORIENTACION SOBRE LA IMPLEMENTACION
A.06.01.01	Roles y responsabilidades de la seguridad de la información	Política General de Seguridad con roles y responsabilidades del SGSI definidos. Resoluciones y/o documento en el que se establezca los respectivos nombramientos. Se deberían indicar las áreas por las que las personas son responsables.
A.06.02.02	Teletrabajo	Las organizaciones que permiten las actividades de teletrabajo deberían emitir una política que define las condiciones y las restricciones del uso del teletrabajo. Se deberían considerar los siguientes asuntos donde se considere aplicable y lo permita la ley

MATRIZ DE RESPONSABILIDADES
POLITÍCA DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

RESPONSABILIDADES	DIRECTORIO	GERENTE GENERAL	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	OFICIAL DE SEGURIDAD DE LA INFORMACIÓN	GERENTES DE ÁREA	AUDITOR INTERNO	RECURSOS HUMANOS Y SERVICIO	USUARIOS
Aprobar la Política de Seguridad de la Información.	X							
Sponsor de la Implementación del SGSI.	X							
Revisar y proponer Política de Seguridad de la Información.		X	X					
Comunicar la Política de Seguridad de la Información.			X	X			X	
Velar por el Cumplimiento de los Controles Internos (procedimientos) relacionados con el SGSI.				X				
Supervigilar que las estrategias definidas por el Directorio, asociadas al control de los activos de información, se desarrollen	X		X	X				

Importancia:
Permite conocer las responsabilidades (deberes y obligaciones) de cada colaborador en la organización, facilitando el ciclo de vida del SGSI

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática



Dominio (7) → Seguridad Ligada a los Recursos Humanos

Política de seguridad ligada a los recursos humanos (PE-SGSI-003), cuyos principales objetivos son:

- Asegurar que todo el personal tiene conocimiento sobre los derechos, deberes y responsabilidades en relación a la seguridad de la información.
- Establecer los niveles de acceso apropiados a la información, brindando y asegurando la confidencialidad, integridad y disponibilidad que requiera cada sistema y usuario.

CONTROL	DESCRIPCIÓN	ORIENTACION SOBRE LA IMPLEMENTACION
A.07.02.02	Concientización, educación en seguridad de la información	Se deberá asegurarse de que los empleados y contratistas están en conocimiento de y que cumplen con sus responsabilidades de seguridad de la información. La dirección debería exigir a todos los empleados y contratistas que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

ANTES DEL EMPLEO	Selección	Términos y Condiciones del Empleo
DURANTE EL EMPLEO	Roles y Responsabilidades respecto de la seguridad	Concientización Educación y Capacitación sobre Seguridad
DESPUÉS DEL EMPLEO	Baja de servicios	

Importancia:
Permite conocer a los usuarios sus deberes, derechos y obligaciones respecto de la seguridad de la información en la organización.

Dominio (8) → Administración de Activos

2do Seminario de Ciberseguridad para funcionarios públicos JUEVES 28/09 2021

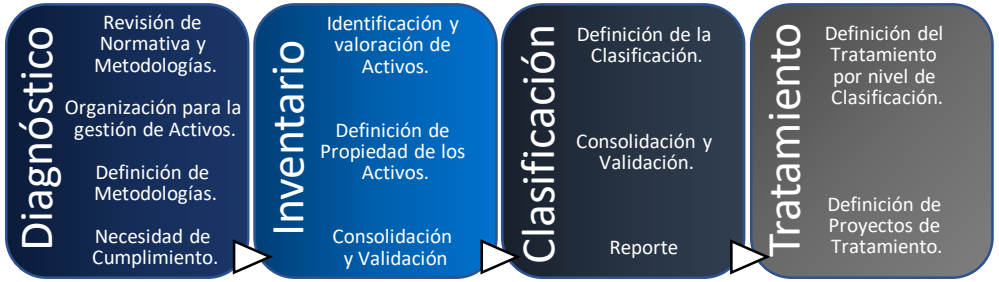
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

✓ **Política de administración de activos de información para usuarios** (PE-SGSI-002) +,
✓ **Procedimiento uso correcto estaciones de trabajo**, cuyos principales objetivos son:

- Mantener un inventario de activos de la información, a cargo de cada Unidad responsable.
- Almacenar, manejar y custodiar los activos de información de acuerdo con su nivel de clasificación.
- Delinear el cuidado especial y responsable que se le debe dar a los computadores institucionales para controlar la administración de este recurso y evitar el mal uso, robo, su posible pérdida o daño.

CONTROL	DESCRIPCIÓN	ORIENTACION SOBRE LA IMPLEMENTACION
A.08.01.01	Inventario de Activos	Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos. Para cada uno de los activos identificados, se debería asignar su propiedad (ver 8.1.2) y clasificación. (Ver 8.2).

GESTIÓN DE ACTIVOS DE INFORMACIÓN



CLASIFICACIÓN SEGÚN CRITICIDAD

SERVICIO	CLASIFICACIÓN	NIVEL DE SERVICIO (SLA)	INDISPONIBILIDAD MES EN HORAS
Serv. Correo	Crítica	99,95%	00:36
Serv. Autentificación AD	Crítica	99,95%	00:36
Servicio de Telefonía	Crítica	99,95%	00:36
Servicio Internet	Crítica	99,95%	00:36
Servicio Erp	Alta	99,80%	01:30
Plat. de Remuneraciones	Media	99,50%	03:30

Importancia:
Permite clasificar los activos y permite determinar el tratamiento que se le dará de acuerdo a su clasificación

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Dominio (9) → Control de Acceso

2do Seminario de Ciberseguridad para funcionarios públicos JUEVES 28/09 2021

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

- ✓ **Política control de acceso** (PE-SGSI-006) **+**,
- ✓ **Procedimiento control gestión de identidad**, cuyos principales objetivos son:
  - Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de estaciones de trabajo.
  - Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.
  - Establecer los niveles de acceso apropiados a la información de la organización, brindando y asegurando la confidencialidad, integridad y disponibilidad que requiera cada sistema y usuario.

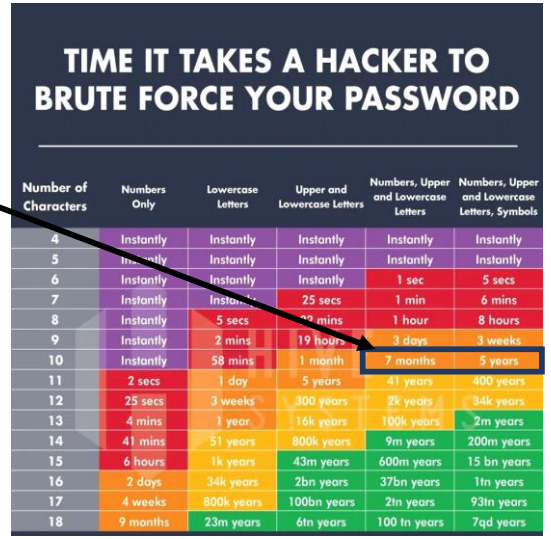
CONTROL	DESCRIPCIÓN	ORIENTACION SOBRE LA IMPLEMENTACION
A.09.01.01	Política de control del acceso	Política de control de acceso físico y lógico alineada a dominios 8, 9 y 18 Se debería implementar un proceso formal de registro y cancelación de registro de un usuario para permitir la asignación de derechos de acceso.
A.09.01.02	Acceso a redes y servicios de red	Procedimiento de acceso a la red alineado a política de control de acceso. Los usuarios solo deberían tener acceso a la red y a los servicios de red en los que cuentan con autorización específica.
A.09.04.03	Sistema de gestión de contraseñas	Procedimiento de sistemas de gestión de contraseñas, alineados a control 9.3.1. Los sistemas de administración de contraseñas deberían ser interactivos y deberían garantizar contraseñas de calidad.

Estructura de la Password recomendada:

- Largo mínimo de 10 caracteres,
- Uso de números obligatorio (1 o más),
- Uso de letras mayúsculas obligatorio (1 o más),
- Uso de letras minúsculas obligatorio (1 o más) y
- Uso de caracteres especiales obligatorio (1 ó más).

Otros parámetros recomendados:

- Cambio automático cada 90 días,
- Al 3° intento fallido bloque x 24 horas.



Importancia:
Permite definir y controlar los accesos correctos y adecuados a los activos de información en la organización.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Dominio (11) → Seguridad Física

2do Seminario de Ciberseguridad para funcionarios públicos JUEVES 28/09 2021

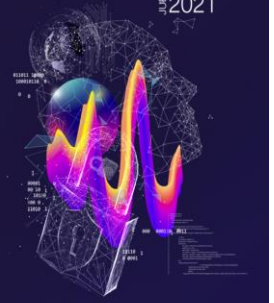
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

- ✓ **Política de seguridad física y del ambiente** (PE-SGSI-004) +
- ✓ **Procedimiento de seguridad física**, cuyos principales objetivos son:
  - Velar por la protección de la Infraestructura tecnológica de almacenamiento de información y de provisión de servicios tecnológicos de apoyo a la gestión.
  - Protección de los espacios Físicos.
  - Dar condiciones de continuidad operacional a la gestión operacional, de servicio y comercial de la organización.

CONTROL	DESCRIPCIÓN	ORIENTACION SOBRE LA IMPLEMENTACION
A.11.01.01	Perímetro de seguridad física	Procedimiento de control de acceso, en concordancia con el Procedimiento de control de acceso físico. Los perímetros de seguridad se deberían definir y utilizar para proteger a las áreas que contienen información y a las instalaciones de procesamiento de información sensible o crítica.

Importancia:
Permite definir y controlar un resguardo adecuado a los activos de información en la organización.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática



Dominio (12 y 13) → Seguridad de las Operaciones y Comunicaciones

- ✓ **Política gestión de comunicaciones y operaciones** (PE-SGSI-005) +,
- ✓ **Procedimiento uso correcto de servidores y redes +,**
- ✓ **Procedimiento prevención de programa malicioso informático +,**
- ✓ **Procedimiento de respaldo y recuperación de la información +,**
- ✓ **Procedimiento uso correcto de servidores y redes** , cuyos principales objetivos son:

- Analizar y establecer una adecuada gestión de comunicaciones y operaciones apropiados para la información de la organización, brindando y asegurando la confidencialidad, integridad y disponibilidad que requiera cada sistema.
- Controlar y asegurar las instalaciones de procesamiento de información y datos de la empresa

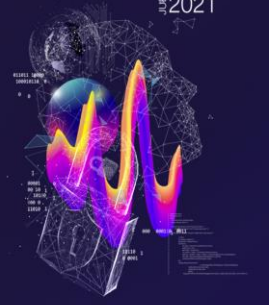
CONTROL	DESCRIPCIÓN	ORIENTACION SOBRE LA IMPLEMENTACION
A.12.02.01	Controles contra códigos maliciosos	Procedimiento contra código malicioso. Se deberían implementar controles para la detección, prevención y recuperación para resguardarse contra el malware en combinación con la concientización adecuada para los usuarios.
A.12.03.01	Respaldo de la información	Políticas de Respaldo. Se deberían realizar copias de la información, del software y de las imágenes del sistema y se deberían probar de manera regular de acuerdo con una política de respaldo acordada.
A.12.05.01	Instalación del software SOP	Procedimiento de instalación de software en los sistemas. Se deberían implementar procedimientos para controlar la instalación de software en sistemas operacionales.
A.12.06.02	Restricciones sobre la instalación de software	Procedimiento o Documento que detalle las Restricciones sobre la instalación de software. Se deberían establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.
A.13.01.01	Controles de Red	Procedimiento o Documento que detalle los controles de red. Se deberían administrar y controlar las redes para proteger la información en los sistemas y aplicaciones. Se debe disponer de un diagrama de Red de Datos de la Organización.

Nota:
Si bien es cierto, la política específica de seguridad de las operaciones y comunicaciones definida y los procedimientos desarrollados (4) cubren 11 controles del dominio 12 y 13 para el propósito de esta presentación sólo se muestran 5.

Importancia:
Permite definir y controlar importantes estándares de operación para la administración en forma adecuada y segura de los activos de información en la organización.

Dominio (14) → Adquisición, desarrollo y mantención del sistema

2do Seminario de Ciberseguridad para funcionarios públicos JUEVES 28/09 2021



Ministerio del Interior y Seguridad Pública
Gobierno de Chile

- ✓ **Política de proceso de desarrollo de software** (PE-SGSI-007) **+**,
- ✓ **Procedimiento uso correcto de servidores y redes +**,
- ✓ **Procedimiento para desarrollo de software**, cuyos principales objetivos son:

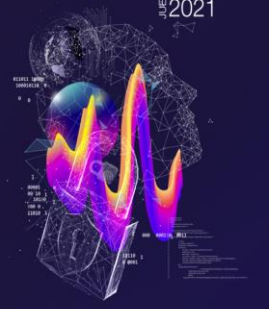
- Identificar los requerimientos de seguridad de cada una de las aplicaciones.
- Identificar toda la información relacionada con las aplicaciones (usuarios y restricciones de acceso, interoperabilidad, reglas de respaldo, disponibilidad y ventanas de trabajo entro otros).
- Establecer los niveles de acceso apropiados a la información institucional, perfil de usuarios.

CONTROL	DESCRIPCIÓN	ORIENTACION SOBRE LA IMPLEMENTACION
A.14.02.01	Política de desarrollo seguro	Política de desarrollo seguro, se deberían establecer reglas para el desarrollo de software y sistemas y, se deberían aplicar a los desarrollos dentro de la organización.
A.14.02.06	Entorno de desarrollo seguro	Procedimiento o Documento que señale el Entorno de desarrollo seguro Las organizaciones deberían establecer y proteger adecuadamente a los entornos de desarrollo seguros para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema.
A.14.02.08	Prueba de seguridad del sistema	Procedimiento o Documento que establezca la metodología de seguridad del sistema. Las pruebas de la funcionalidad de seguridad se deberían realizar durante el desarrollo y debe estar especificadas en el procedimiento.
A.14.02.09	Prueba de aprobación del sistema	Procedimiento o Documento que establezca las pruebas de aprobación del sistema Se deberían establecer programas de pruebas de aceptación por parte de los clientes y criterios relacionados para los nuevos sistemas de información, actualizaciones y nuevas versiones.

Nota:
Si bien es cierto, la política específica de proceso de desarrollo de software definida y el procedimiento desarrollado (1) cubren 6 controles del dominio 14 para el propósito de esta presentación sólo se muestran 4.

Importancia:
Permite establecer controles adecuados requeridos para el desarrollo de software en las organizaciones, estos controles evitan costos mayores asociados al ciclo de vida de los desarrollos.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática



Dominio (15) → Relaciones con el proveedor

Procedimiento de tercerización de servicios TI, cuyos principal objetivo ES:

- Definir las actividades y las acciones que permitan definir, guiar, formalizar y administrar los procesos de entregar a terceros la responsabilidad por la ejecución de tareas correspondientes a la entrega, uso y aplicación de tecnologías de la información (Outsourcing), en la empresa y sus unidades dependientes.

CONTROL	DESCRIPCIÓN	ORIENTACION SOBRE LA IMPLEMENTACION
A.15.02.01	Supervisión y revisión de los servicios del proveedor	Procedimiento o Documento que detalle los mecanismos de Supervisión y revisión de los servicios del proveedor Las organizaciones deberían monitorear, revisar y auditar la presentación de servicios del proveedor de manera regular.

CUMPLIMIENTO SLA 2021 VARIOS PROVEEDORES															
PLATAFORMA	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	SLA OBJETIVO	SLA 2020	SLA 2019
ERP	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%				99,50%	100,00%	100,00%
Infraestructura	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%				95,00%	100,00%	100,00%
Respaldo	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%				98,00%	100,00%	100,00%
Correo	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%				99,90%	100,00%	100,00%
Telefonía	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%				99,90%	100,00%	100,00%
Enlaces	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%				99,90%	100,00%	100,00%

Importancia:
Permite establecer controles adecuados requeridos para la operación de servicios externalizados, permite control de SLA definidos.

Dominio (16) → Gestión de Incidentes de seguridad de la información

2do Seminario de Ciberseguridad para funcionarios públicos
JUEVES 28/09 2021

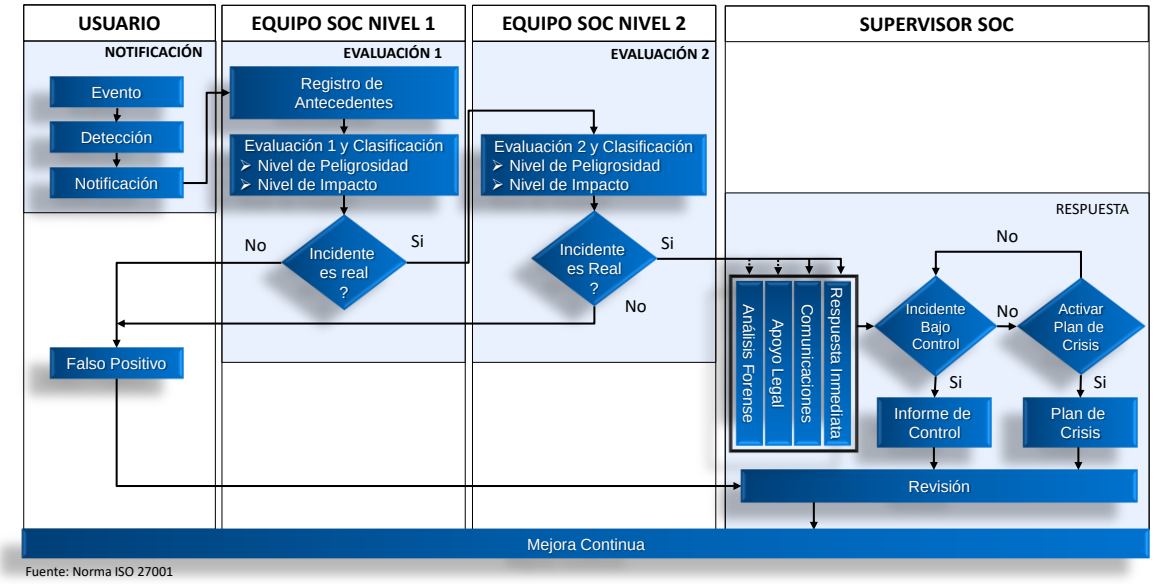
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

✓ **Política gestión de incidentes de seguridad de la información** (PE-SGSU-008) +,
✓ **Procedimiento gestion de incidentes**, cuyos principales objetivos son:

- Responder en forma rápida, eficaz y ordenada ante la ocurrencia de incidentes de seguridad que afecten los activos de información de la organización.
- Asegurar un enfoque consistente y eficaz sobre la gestión de los incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades (educación).

CONTROL	DESCRIPCIÓN	ORIENTACION SOBRE LA IMPLEMENTACION
A.16.01.02	Informe de eventos de seguridad de la información	Procedimientos de gestión de incidentes de seguridad de la información. Los eventos de seguridad de la información se deberían informar a través de canales de administración adecuados lo más pronto posible.
A.16.01.05	Respuesta ante incidentes de seguridad de la información	Procedimiento que indique como responder ante incidentes de seguridad de la información. Se debería responder ante los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.

Modo de Operación Control de Incidentes CSIRT



Fuente: Norma ISO 27001

Importancia:
Permite establecer un estándar de operación y de servicio respecto de la gestión de incidentes sobre los activos de información.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

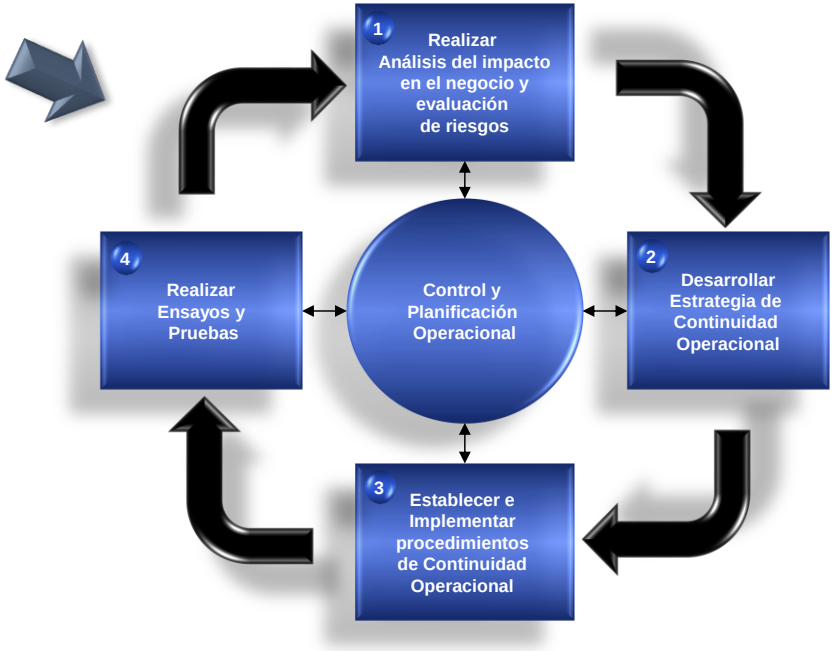
Dominio (17) → Gestión de la continuidad del Negocio

Política de planificación de la continuidad de la seguridad de la información (PE-SGSI-010), cuyo principal objetivo es:

- Es brindar una guía que permita, al personal designado por el departamento de TI gestionar de mejor forma el desempeño diario de las tareas que involucran los activos de información de acuerdo con la normativa vigente, respecto de contingencias catastróficas o emergencias que impidan la operación normal de las plataformas tecnológicas.

CONTROL	DESCRIPCIÓN	ORIENTACION SOBRE LA IMPLEMENTACION
A.17.01.01	Planificación de la continuidad de la seguridad de la información	Política que señale la Planificación de la continuidad de la seguridad de la información. La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la administración de la seguridad de la información ante situaciones adversas, es decir, durante una crisis o desastre.

Pasos a seguir para implementar un Plan de Continuidad Operacional



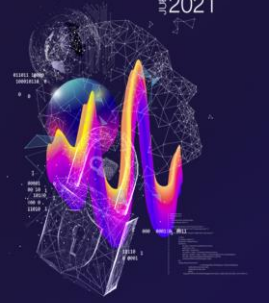
Ejemplo que hacer cuando ocurre:

- Pérdida de suministro de energía eléctrica
- Corte en los enlaces de comunicaciones
- Falla en los equipos de comunicaciones
- Ataque de virus informático
- Falla operacional site principal
- Operación bajo situación de Fuerza Mayor

Importancia:
Permite establecer una guía de como operar ante la ocurrencia de un incidente en la organización, asignado roles y responsabilidades. Se recomienda iniciar con los más comunes.

Dominio (18) → Cumplimiento

2do Seminario de Ciberseguridad para funcionarios públicos JUEVES 28/09 2021



Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Procedimiento de revisión de cumplimiento técnico, cuyos principal objetivo es:

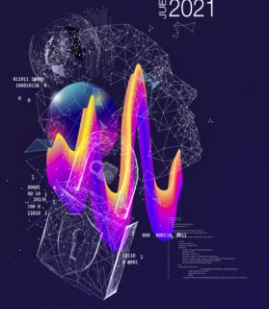
- Contar con un mecanismo adecuado para la revisión del cumplimiento técnico de los controles implementados por parte de la organización. Esta revisión corresponderá al estado de avance porcentual del cumplimiento de cada uno de los controles registrados en la planilla de control del cumplimiento técnico.

CONTROL	DESCRIPCIÓN	ORIENTACION SOBRE LA IMPLEMENTACION
A.18.02.01	Revisión independiente de la seguridad de la Información	Procedimiento o Documento que detalle el mecanismo de revisión independiente de la información de seguridad de la Información.
A.18.02.03	Verificación del cumplimiento técnico	Procedimiento o Documento que indique como se debería revisar y verificar regularmente el cumplimiento técnico de las políticas y normas de seguridad de la Información.

PLANILLA DE CONTROL DEL CUMPLIMIENTO TECNICO NORMA ISO27002				
N°	CONTROL	DECRIPCION CONTROL	ORIENTACION SOBRE LA IMPLEMENTACION	DOCUMENTACION O EVIDENCIA REQUERIDA
1	A.05.01.01	Políticas para la seguridad de la información	En el nivel más alto, las organizaciones deberían definir una "política de seguridad de la información" que la apruebe la dirección y que establece el enfoque de la organización para administrar sus objetivos de seguridad de la información.	1. EXISTENCIA DE POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION 2. EXISTENCIA DE RESOLUCION 3. EVIDENCIA DE DIFUSIÓN
2	A 05.01.02	Revisión de las Politicas de Seguridad de la Información	Cada política debería tener un titular que tenga responsabilidad administrativa aprobada para el desarrollo, la revisión y la evaluación de ellas. La revisión debería incluir la evaluación de oportunidades de mejora y un enfoque para administrar la seguridad de la información en respuesta a los cambios en el entorno que las puedan afectar. Se debería obtener la aprobación de la dirección para una política revisada.	1. EXISTENCIA DE POLITICAS Y PROCEDIMIENTOS 2. ACTA COMITÉ DE RIESGO APROBACION DE POLITICAS Y PROCEDIMIENTOS 3. ACTA DE CONSTITUCION DE COMITÉ DE SEGURIDAD 4. ACTA NOMBRAMIENTO DE ENCARGADO DE SEGURIDAD 5. RESOLUCION EXENTA N°4468 6. RESOLUCION EXENTA N°555
3	A.06.01.01	Roles y responsabilidades de la seguridad de la información	Política General de Seguridad con roles y responsabilidades del SGSI definidos. Resoluciones y/o documento en el que se establezca los respectivos nombramientos. Se deberían indicar las áreas por las que las personas son responsables.	1. EXISTENCIA DE POLITICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN 2. EXISTENCIA DE UNA POLITICA DE ROLES U ORGANICA DE LAS POLITICAS 3. ACTA COMITÉ DE RIESGO APROBACION DE POLITICAS Y PROCEDIMIENTOS 4. RESOLUCION EXENTA N°555
4	A.07.02.02	Concientización, educación en seguridad de la información	Se deberá segurarse de que los empleados y contratistas están en conocimiento de y que cumplen con sus responsabilidades de seguridad de la información. La dirección debería exigir a todos los empleados y contratistas que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.	1. EXISTENCIA DE UNA POLITICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN 2. ACTA COMITÉ DE RIESGO APROBACION DE POLITICAS Y PROCEDIMIENTOS 3. RESOLUCION EXENTA N°555 4. EVIDENCIA DE DIFUSION Y CAPACITACION

Importancia:
Permite asegurar un funcionamiento adecuando e incorporar mejora continua al Sistema de Gestión de Seguridad de la Información (SGSI)

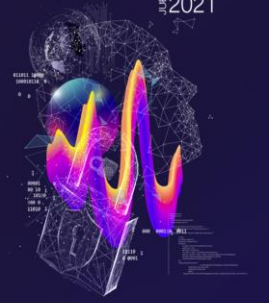
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática



Ejemplo de ataque de Spearphishing (Fraude del CEO)

A continuación se muestra un ejemplo de un Phishing dirigido a una sociedad que cuenta con un SGSI implementado y que tiene controles definidos que le permiten atenuar y evitar potenciales fraudes.

2do Seminario de Ciberseguridad para funcionarios públicos JUEVES 28/09 2021



Ejemplo de ataque de Spearphishing (Fraude del CEO)

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

[redacted]

Santiago, 14 de Septiembre de 2021

REF: SOLICITUD DE FONDO PARA INVERSION EN EL EXTRANJERO POR USD$ [redacted]

De mi consideración:

Por medio de la presente y de acuerdo con lo conversado y autorizado favor solicito a Uds. realizar abono a la cuenta corriente N° [redacted] de la sociedad Alerce Blanco la suma de USD$ [redacted]

Capital Comprometido del Proyecto: [redacted]

Capital Depositado a la fecha: [redacted]

Caja Disponible a la fecha: [redacted]

Esta transferencia requiere sea realizada a más tardar el 15 de Septiembre, con el propósito de obtener un mejor rentabilidad en la transacción.

Los datos para realizar la transferencia bancaria son los siguientes:

Banco del Beneficiario	: UOB BANK OF SINGAPORE
Dirección Banco Beneficiario	: 80 Raffles Place UOB Plaza 1, #07-01, Singapore 048624
SWIFT CODE	: [redacted]
Beneficiario	: UNITES SEA HOLDING PTE LTD
Account Number	: [redacted]
Dirección	: 340 Plaza Park Blvd. Suit 200

[redacted]

Secuencia de eventos:

1. Se obtiene credencial de usuario (Posible Phishing o credencial débil).
2. Se interviene correo creando regla específica que captura correos.
3. Se crean cuentas de correo falsas con extensión ".xx"
4. Maleantes detectan envío de documentos de transferencia de fondos.
5. Se interviene PDF cambiando cuenta de destino de la transferencia.
6. Gracias a validaciones técnicas y manuales se evita estafa (Fraude del CEO).

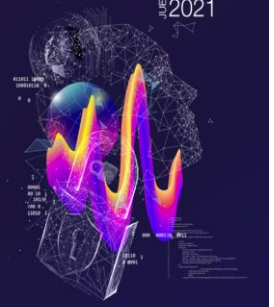
¿Qué es el fraude del CEO o BEC?

El fraude del CEO es una forma de ataque de ***Spearphishing*** que apunta a los miembros del equipo financiero o contable de una compañía, en el caso de este fraude, los criminales intentan hacerse pasar por ejecutivos para convencer a los destinatarios del correo electrónico de la necesidad de realizar una transferencia de dinero de forma urgente para una operación supuestamente crítica para la organización. Sin embargo, el dinero se transfiere a una cuenta que está bajo el control de los atacantes. El FBI estima que entre 2016 y 2019, se generaron pérdidas por MMUSD$ 26.000 a través de ataques conocidos como BEC (del inglés, Business Email Compromise).

Conclusión:

- ✓ Construir claves robustas y difíciles de deducir.
- ✓ Informar a Soporte TI de potenciales Phishing o actividades extrañas.
- ✓ Revisar reglas existentes en nuestros correos, generar acciones de mitigación.
- ✓ Mantener precaución en la información que se comparte.
- ✓ Potenciar uso de firma electrónica entre involucrados.
- ✓ Mantener estrictos controles manuales sobre operaciones financieras.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática



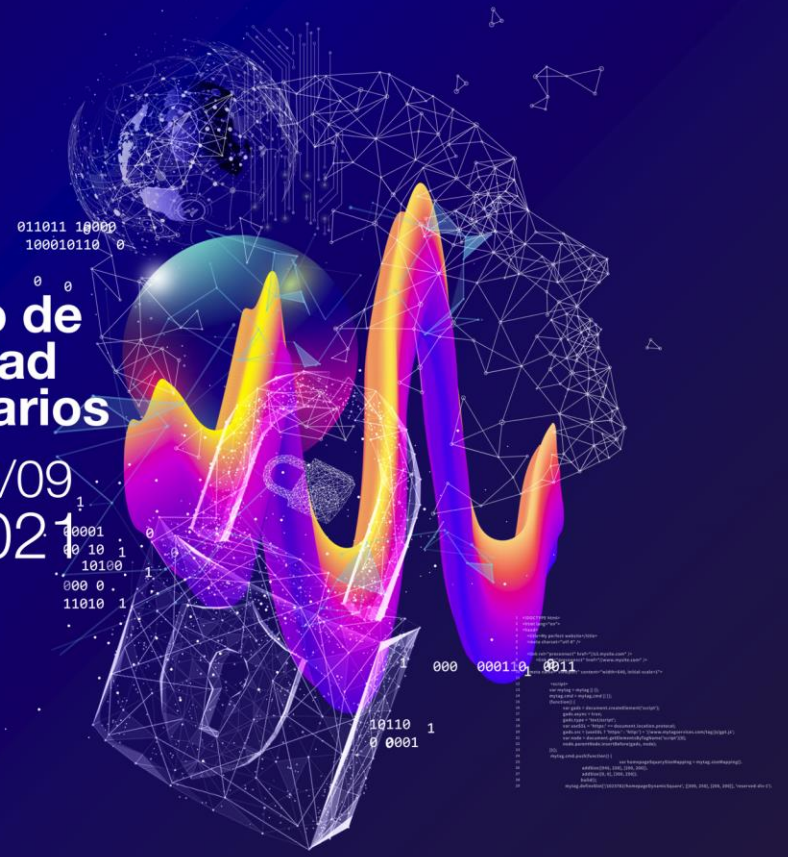
Por qué es necesario implementar Políticas y Procedimientos de Seguridad ?

- ***Porque el contar con regulaciones adecuadas y conocidas, permitirá reducir los riesgos de seguridad y mejorar el nivel de madurez tecnológica de la organización.***

- ***Capacitar, Capacitar, Capacitar:***
  Si bien es cierto las organizaciones cuenta con herramientas tecnológicas (AntiSpam y Antivirus) que nos protegen de posibles ataques externos, es de suma importancia que se entienda que:
  "la primera barrera de contención somos nosotros mismos".

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021



Ministerio del Interior y Seguridad Pública
Gobierno de Chile

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT
https://www.csirt.gob.cl/

Teatinos 92 piso 6
Santiago, Chile