Conceptos necesarios para entender la Ciberseguridad

Hernán Espinoza
Asesor CSIRT
Coordinación Nacional de Ciberseguridad
Mes de la Ciberseguridad de 2023

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

CSIRT

CSIRT es el acrónimo de "Equipo de Respuesta ante Incidencias de Seguridad Informática". En español, también se puede utilizar el término "CERT", que significa "Centro de Respuesta a Emergencias Informáticas".

Un CSIRT es un grupo de profesionales de la Ciberseguridad que se encarga de responder a incidentes de seguridad informática. Estos incidentes pueden ser muy variados, desde ataques de malware hasta violaciones de datos.

Las funciones principales de un CSIRT son:

- Recibir y analizar informes de incidentes.
- Investigar y responder a incidentes.
- Ofrecer asistencia técnica a las víctimas de incidentes.
- Comunicar información sobre incidentes a las partes interesadas.

CSIRT

Los CSIRT pueden ser públicos o privados. Los CSIRT públicos suelen ser financiados por el gobierno o por organizaciones sin ánimo de lucro. Los CSIRT privados suelen ser contratados por empresas o organizaciones para proporcionar servicios de respuesta a incidentes.

En Chile tenemos el CSIRT de Gobierno:

www.csirt.gob.cl

CSIRT

Los CSIRT juegan un papel fundamental en la protección de la Ciberseguridad.

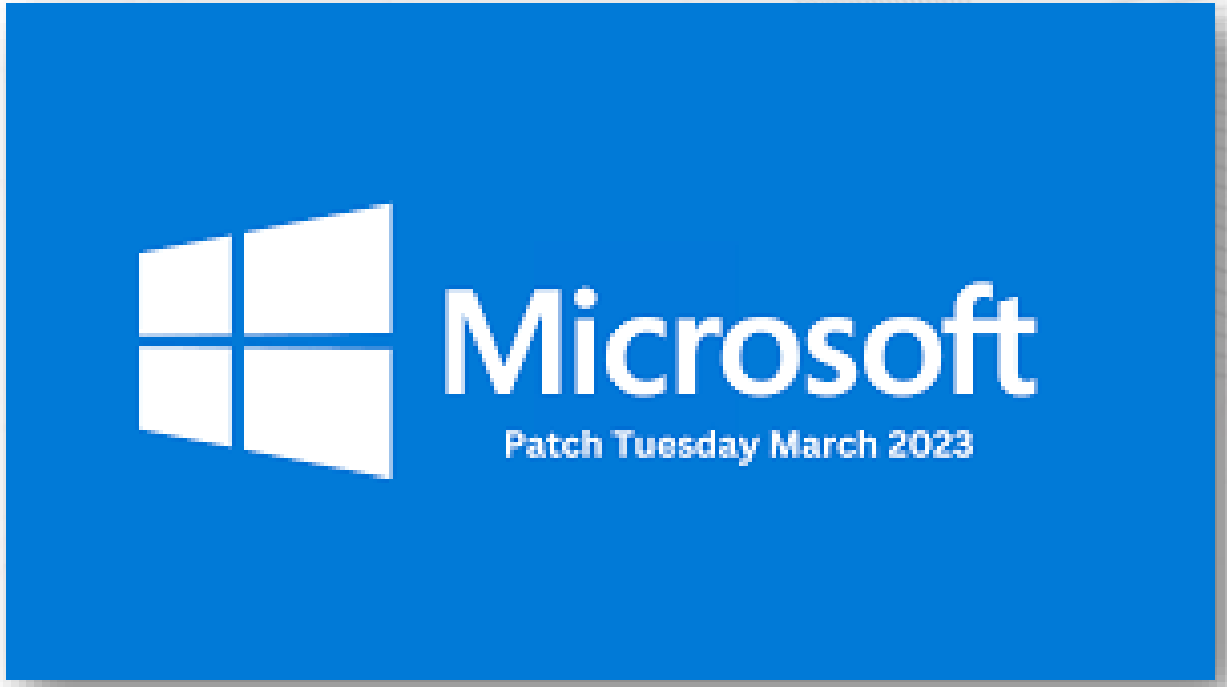
Su trabajo ayuda a prevenir, detectar y responder a incidentes de seguridad informática, lo que contribuye a proteger los sistemas y datos de las organizaciones y los ciudadanos.

Preguntas

- ¿PASA ALGO TODOS LOS SEGUNDOS MARTES DE CADA MES?

Preguntas

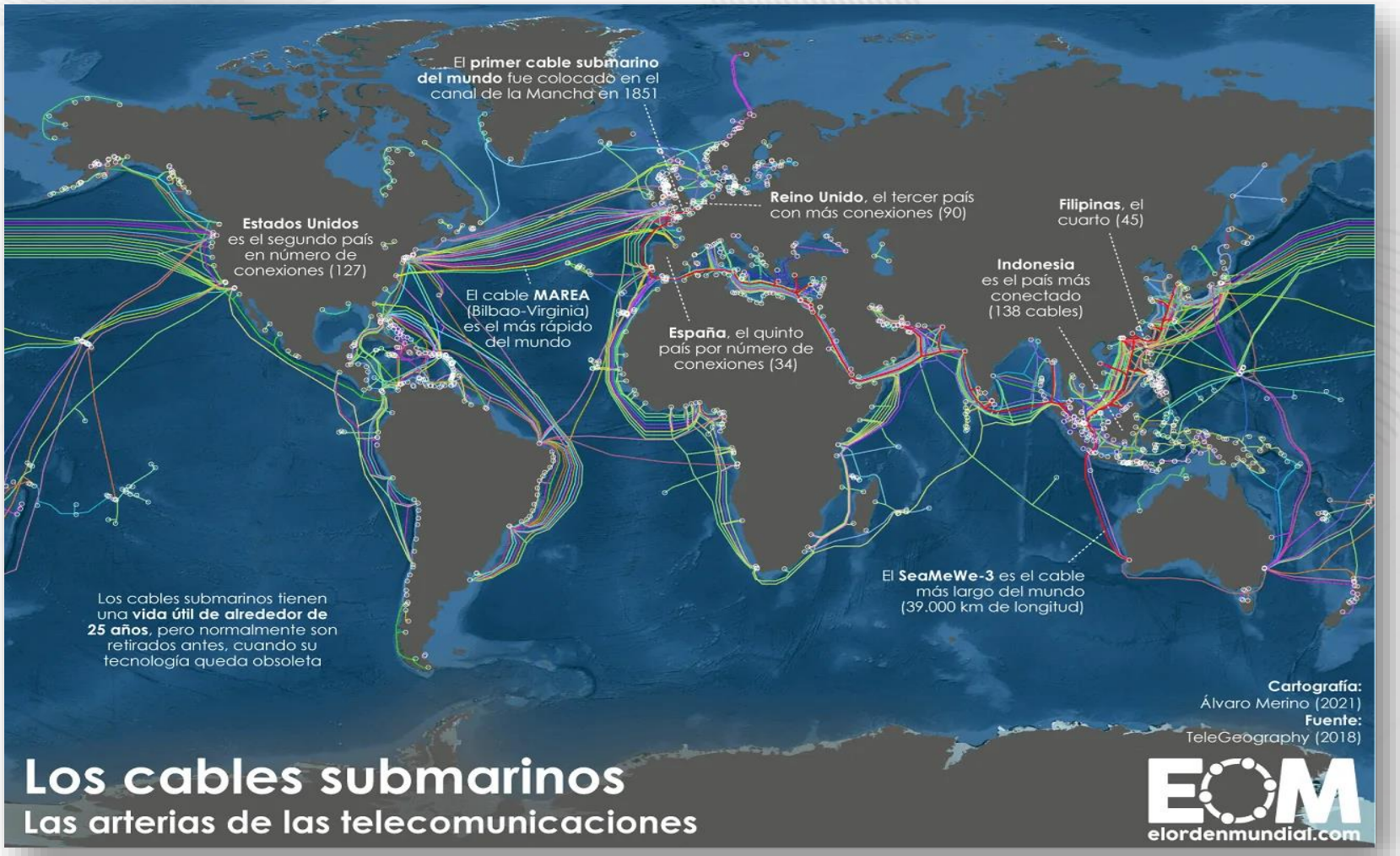
- ¿PASA ALGO TODOS LOS SEGUNDOS MARTES DE CADA MES?



Preguntas

- ¿TODOS PARCHARON SUS COMPUTADORES O SABEN SI SE HACE EN LA INSTITUCIÓN DONDE TRABAJA?

¿Estamos en una isla?



DISTANCIA

A 1 Click

A Milisegundos

ALERTA IA

- La inteligencia artificial (IA) es la capacidad de las máquinas para aprender y actuar de manera inteligente. Esto incluye la capacidad de entender el mundo que les rodea, tomar decisiones y resolver problemas.

- No perdamos de vista que la IA está avanzando a pasos agigantados y comenzará a tomarse muchos espacios tradicionales de múltiples labores.

- **La ciberseguridad NO se escapa a esto.**

ALERTA IA

Algunos temas sobre los que la IA mostrará sus enormes capacidades más pronto de lo que esperamos:

- Recopilar y etiquetar datos de los ciberdefensores para formar agentes de ciberseguridad defensivos.
- Detectar y mitigar las tácticas de ingeniería social.
- Automatizar el “TRIAGE” de incidentes.
- Identificar problemas de seguridad en el código fuente.
- Asistir en el análisis forense de redes o dispositivos.
- Parchear vulnerabilidades automáticamente.
- Optimizar los procesos de gestión de parches para mejorar la priorización, programación y despliegue de actualizaciones de seguridad.

ALERTA IA

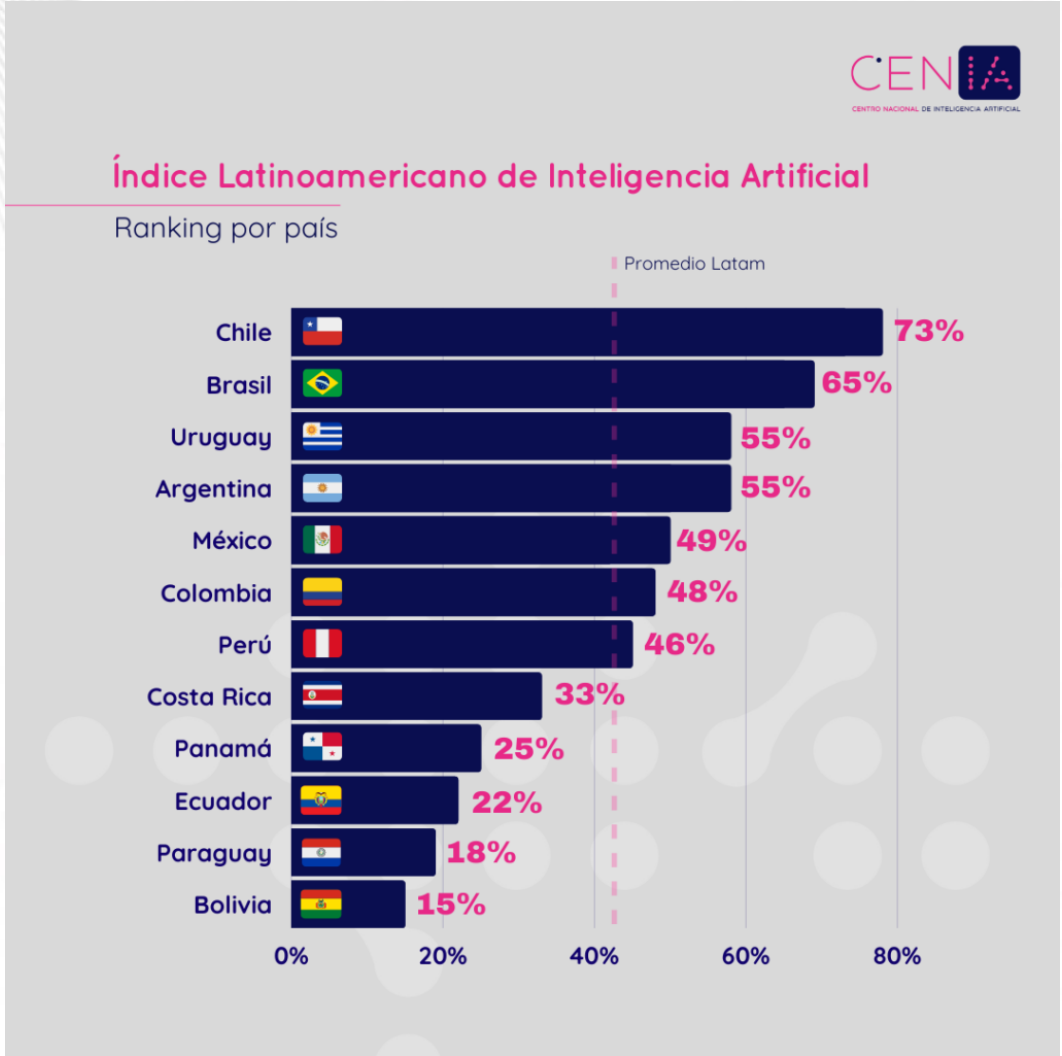
Así que sin ser apocalípticos, es necesario tener en cuenta lo que viene e irnos preparando.

- ¿Cuál será nuestro rol como PERSONAS Y TRABAJADORES en un escenario altamente automatizado y potenciado por las IA?

- ¿Cuál será nuestro rol como usuarios?

ALERTA IA

"Chile sobresale como referente regional en diferentes aspectos. Entre las áreas en las que se destaca encontramos infraestructura, formación profesional, capital humano avanzado, investigación, adopción y en casi todos los subindicadores de la dimensión de gobernanza"



Fuente: https://www.cenia.cl/2023/08/16/latinoamerica-que-tan-preparados-estamos-para-la-inteligencia-artificial-estudio-liderado-por-cenia-revela-importantes-hallazgos/

ALERTA IA

https://minciencia.gob.cl/areas/inteligencia-artificial/politica-nacional-de-inteligencia-artificial/

Ministerio de Ciencia, Tecnología, Conocimiento e Innovación

Inicio | Ministerio | Macrozonas | Áreas | Noticias | Prensa | Contacto | Biblioteca

Inicio ▸ Política Nacional de Inteligencia Artificial

Política Nacional de Inteligencia Artificial

Presentación | ¿En qué consiste la Política de IA? | Proceso de elaboración

Esta política contiene los lineamientos estratégicos que debe seguir el país en esta materia durante los próximos 10 años con el objetivo de empoderar a las personas en el uso y desarrollo de herramientas de IA, y participar en el debate sobre sus consecuencias legales, éticas, sociales y económicas.

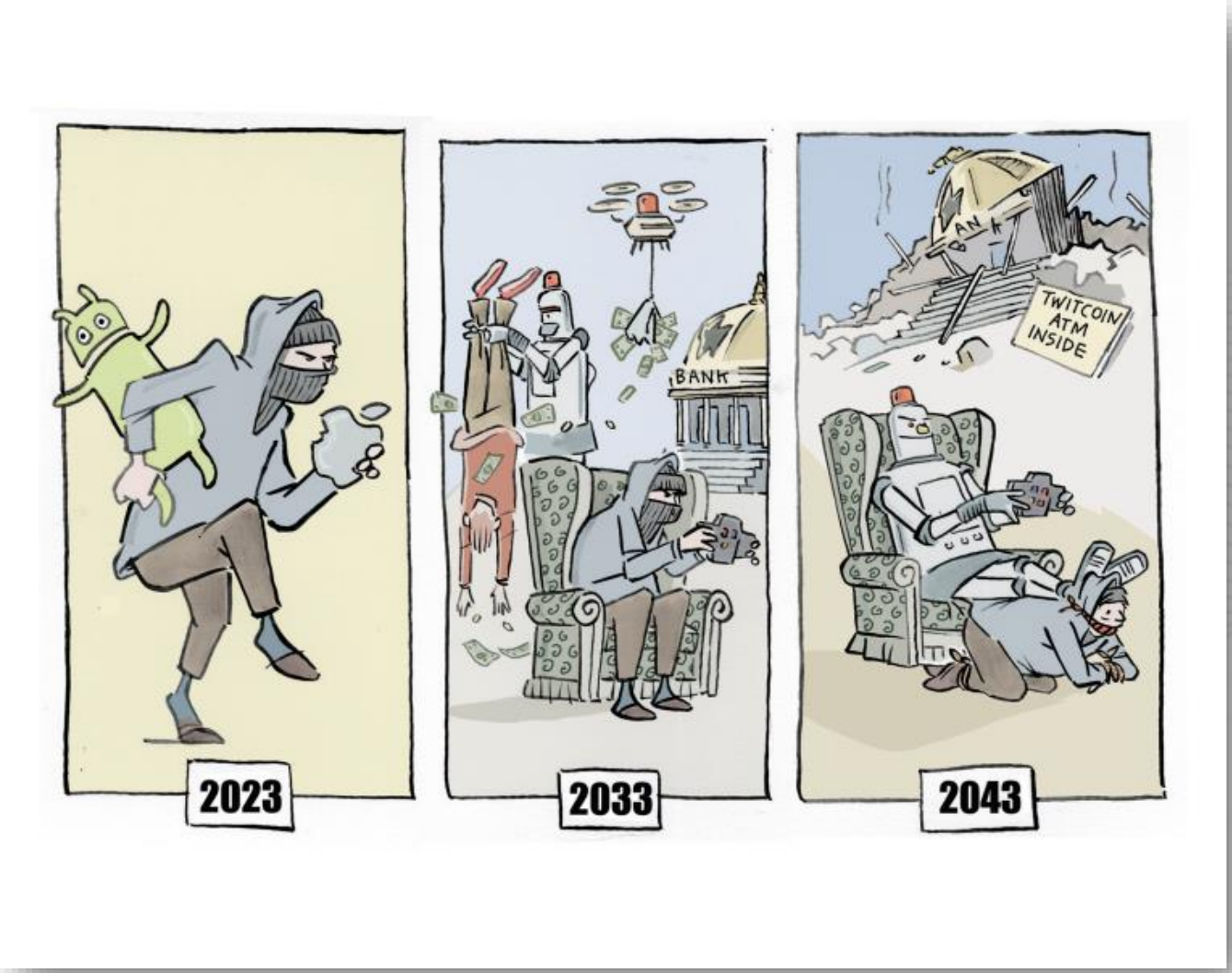
Esta hoja de ruta está construida en torno a tres ejes: factores habilitantes, uso y desarrollo de Inteligencia Artificial en Chile y aspectos de ética y seguridad.

El Plan de Acción que acompaña a esta política reúne **70 acciones prioritarias y 180 iniciativas que se desarrollarán en el periodo 2021-2030.**

Descarga aquí la Política Nacional de IA

Fuente: https://minciencia.gob.cl/areas/inteligencia-artificial/politica-nacional-de-inteligencia-artificial/

ALERTA IA



ALERTA ICS

Los incidentes pueden ocurrir en todas las industrias

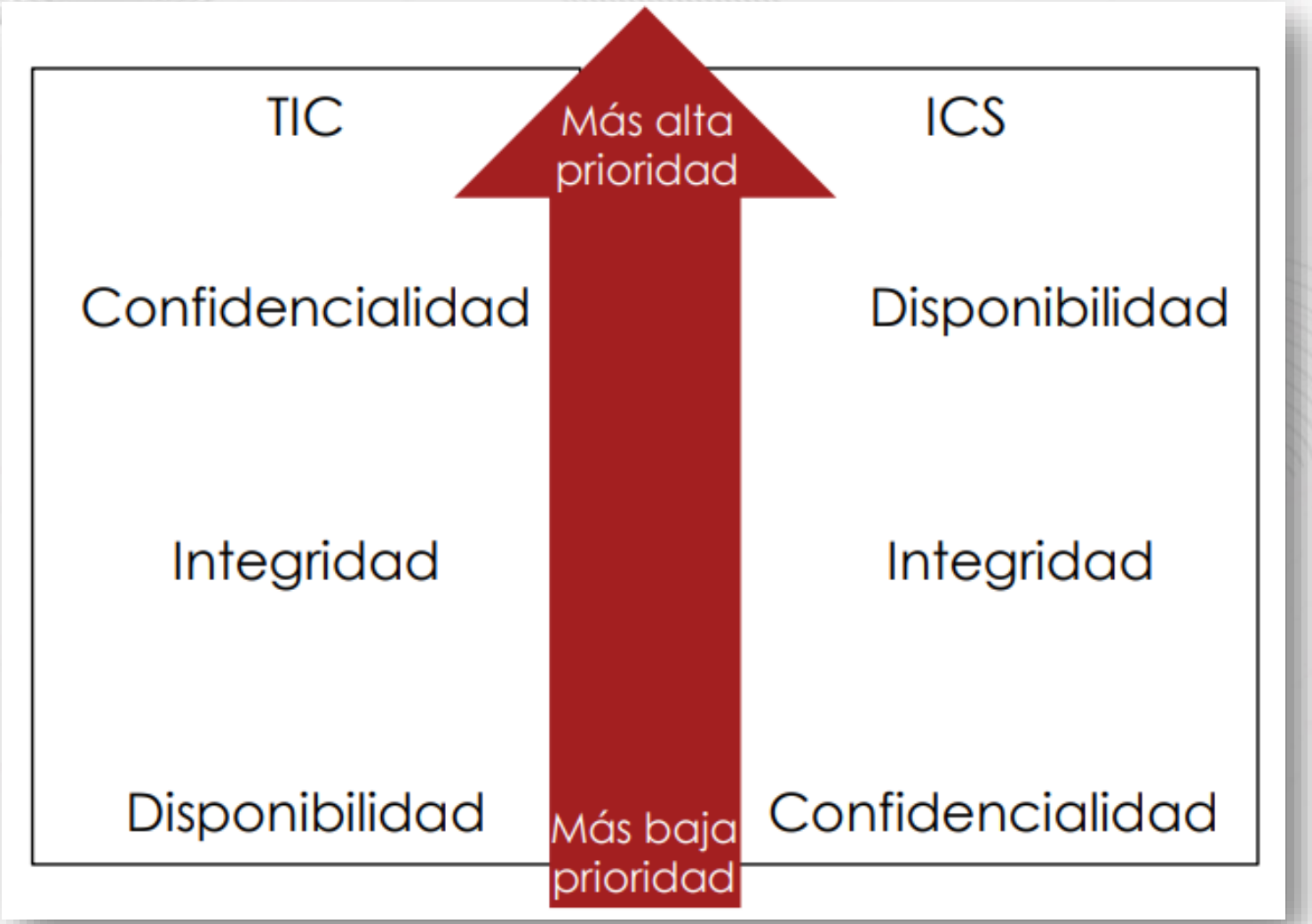
- Es decir pueden afectar a los entornos TI y a los entornos TO.
- TIC o TI: Tecnologías de la Información
- ICS o TO: Tecnologías de la Operación

ES IMPORTANTE QUE SEAMOS CONSCIENTES QUE EN LAS EMPRESAS DE **SERVICIOS ESENCIALES** HAY MUCHA TECNOLOGÍA DE LA OPERACIÓN Y SISTEMAS DE CONTROL INDUSTRIAL QUE DE SER AFECTADOS PUEDEN PRODUCIR UN IMPORTANTE IMPACTO EN LA SOCIEDAD Y SU ECONOMÍA.

ALERTA ICS

- Un sistema de control industrial (**ICS)** es simplemente una serie de dispositivos que se utilizan para regular los datos ingresados en un proceso controlado que generará un resultado deseado.
- En complemento, un ICS esta conformado por un conjunto de dispositivos que administran, comandan, monitorean, dirigen o regulan el comportamiento de otros dispositivos o sistemas en procesos industriales o incluso procesos del sector salud.
- Dispositivos que puede influir sobre el "mundo real".
- **Un sistema que une lo cibernético con lo físico (sensor / actuador).**

ALERTA ICS


TIC
ICS
Más alta prioridad
Confidencialidad
Disponibilidad
Integridad
Integridad
Disponibilidad
Confidencialidad
Más baja prioridad

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Conceptos necesarios para entender la Ciberseguridad

La ciberseguridad es un esfuerzo continuo: Las organizaciones deben implementar medidas de seguridad para proteger sus activos de información.

Sin embargo, estas medidas no son perfectas y no pueden garantizar la seguridad total. Las organizaciones también deben estar preparadas para responder a los ciberataques que se produzcan.

SGSI

De acuerdo con la norma ISO 27001, un **Sistema de Gestión de Seguridad de la Información (SGSI)** es un conjunto de políticas, procedimientos y directrices, junto con los recursos y actividades asociados, que son administrados colectivamente por una organización, en la búsqueda de **proteger sus activos de información esenciales.**

La norma ISO 27001 define un SGSI como "un conjunto de procesos, procedimientos y controles que están diseñados para proteger la información de una organización de **amenazas internas y externas**".

SGSI

Los objetivos principales de un SGSI son:

- ✓ Proteger la confidencialidad, integridad y disponibilidad de la información.
- ✓ Reducir el riesgo de pérdida, acceso no autorizado, uso indebido, divulgación, alteración o destrucción de la información.
- ✓ Cumplir con los requisitos legales y reglamentarios aplicables.
- ✓ Mejorar la eficiencia y eficacia de los procesos de la organización.

SGSI

La norma ISO 27001 proporciona un marco para la implementación de un SGSI eficaz. Este marco se basa en los siguientes principios:

- ✓ Liderazgo y compromiso: la dirección de la organización debe ser responsable de la seguridad de la información.
- ✓ Planificación: la organización debe planificar su enfoque para la gestión de la seguridad de la información.
- ✓ Implementación y operación: la organización debe implementar las medidas de seguridad necesarias para proteger su información.
- ✓ Monitoreo, medición, análisis y evaluación: la organización debe monitorear, medir y analizar su SGSI para garantizar su eficacia.
- ✓ Revisión y mejora continua: la organización debe revisar y mejorar continuamente su SGSI.

SGSI

Los beneficios de implementar un SGSI basado en la norma ISO 27001 incluyen:

- ✓ Protección de la información confidencial de la organización.
- ✓ Reducción del riesgo de pérdida de negocio.
- ✓ Mejora de la confianza de los clientes y socios.
- ✓ Cumplimiento de los requisitos legales y reglamentarios.
- ✓ Mejora de la eficiencia y eficacia de los procesos.

La implementación de un SGSI es un proceso complejo que requiere la participación de todos los niveles de la organización. Sin embargo, los beneficios de implementar un SGSI son significativos y pueden ayudar a las organizaciones a proteger su información y mejorar su posición competitiva.

Fuente: www.iso27000.es/sgsi.html

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

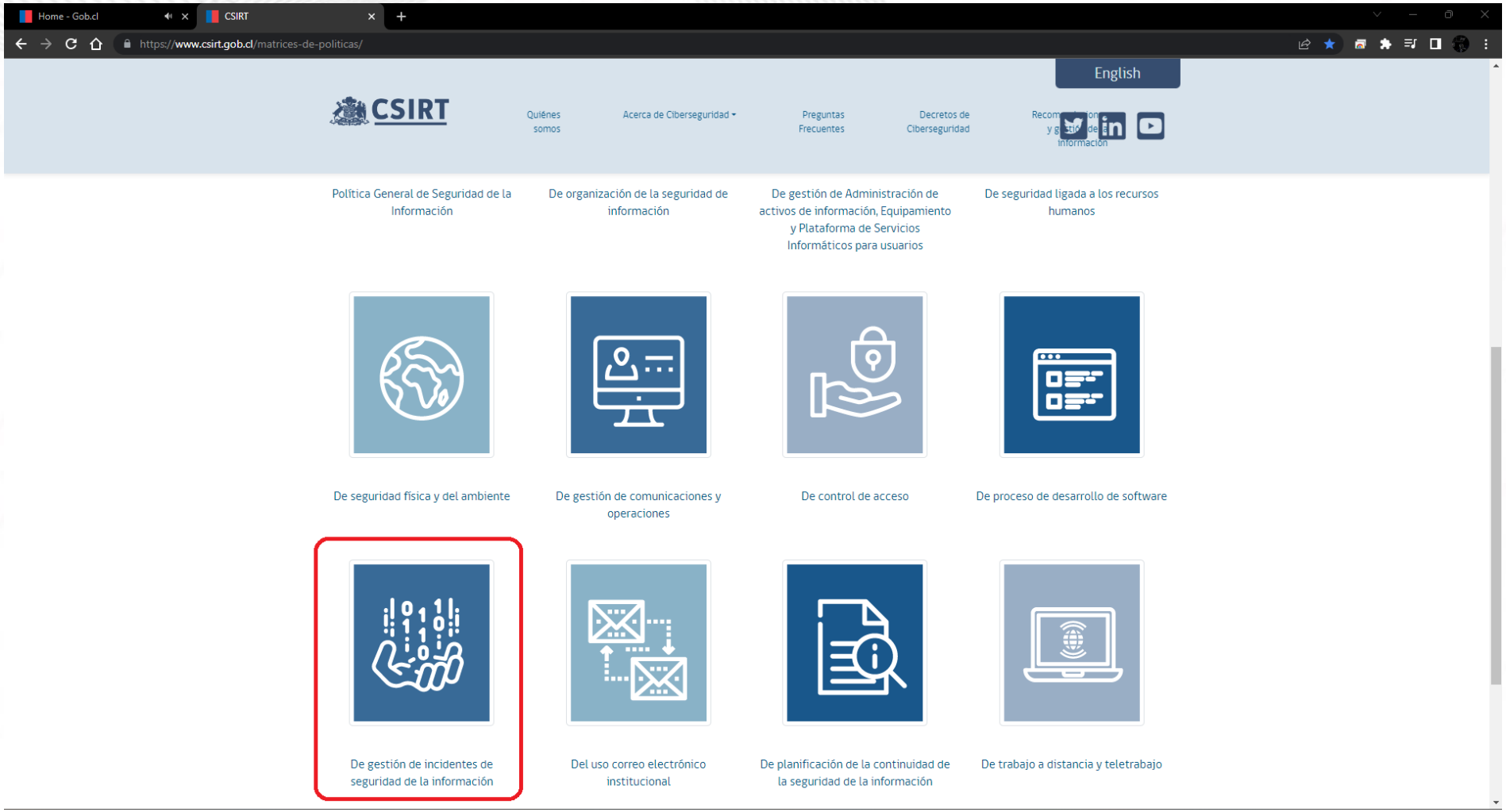
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Son un conjunto de reglas, directivas, derechos y obligaciones que ayudan a prevenir incidentes.

- No son infalibles. Son un ayuda para mitigar riesgos.
- Se apoyan con controles tecnológicos y buenas prácticas.
- Es importante respetarlas e instruirnos en aquellas que nos competen.
- Si detectamos problemas es necesario comunicarlos a nuestro encargado de Ciberseguridad.
- En lo posible, si se abren los espacios institucionales para participar en la mejora de estos instrumentos: **¡Participemos!**
- Su opinión importa. Todos somos parte de la solución.
- Busquen las Políticas de SI en la institución, léalas…

- El Encargados de ciberseguridad cumple un rol relevante en relación a estos instrumentos normativos.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN



AMENAZAS: ¿QUE PUEDEN AFECTAR?

Al pensar en mis **activos de información** o en los de la organización, es importante enfocarse en aquellos activos y procesos institucionales **críticos**.

Un activo puede ser físico o lógico:

- Una planilla Excel, una base de datos, un servidor, un datacenter, una persona, etc.

¿Dónde están expresados estos activos?:

- En las P… de S… de la I…, específicamente en el inventario de activos de información.

¿Dónde está la priorización de productos estratégicos?:

- En las Instituciones Públicas está en el Formulario A1.

¿Dónde está la priorización de activos versus riesgos?

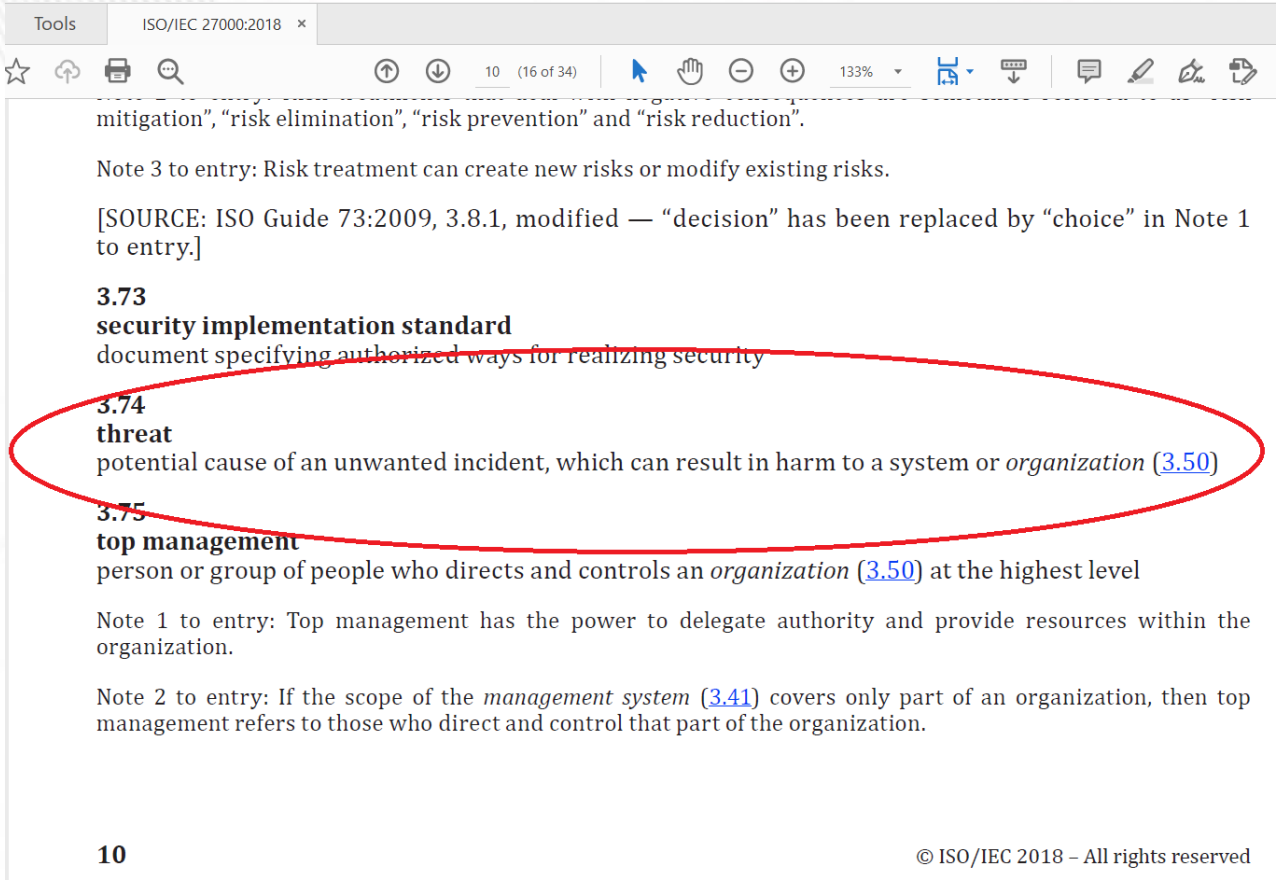
- Proceso de Gestión de Riesgos.

AMENAZAS: AVENTUREMOS UNA DEFINICIÓN

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Según ISO27000

Causa potencial de un incidente no deseado, que puede provocar daños en un sistema u organización


Tools ISO/IEC 27000:2018 ×

10 (16 of 34) 133%

mitigation", "risk elimination", "risk prevention" and "risk reduction".

Note 3 to entry: Risk treatment can create new risks or modify existing risks.

[SOURCE: ISO Guide 73:2009, 3.8.1, modified — "decision" has been replaced by "choice" in Note 1 to entry.]

3.73
security implementation standard
document specifying authorized ways for realizing security

3.74
threat
potential cause of an unwanted incident, which can result in harm to a system or *organization* (3.50)

3.75
top management
person or group of people who directs and controls an *organization* (3.50) at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization.

Note 2 to entry: If the scope of the *management system* (3.41) covers only part of an organization, then top management refers to those who direct and control that part of the organization.

AMENAZAS: MIS PRODUCTOS ESTRATÉGICOS

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

FICHA DE DEFINICIONES ESTRATÉGICAS AÑO 2019-2022 (Formulario A1) 2021

MINISTERIO	MINISTERIO DE RELACIONES EXTERIORES	PARTIDA	06
SERVICIO	SUBSECRETARIA DE RELACIONES ECONOMICAS INTERNACIONALES	CAPITULO	06

Ley orgánica o Decreto que la rige

Ley N° 21.080 de 2018, que modifica diversos cuerpos legales con el objeto de modernizar el Ministerio de Relaciones Exteriores; Decreto con Fuerza de Ley N° 2 de 2019, del Ministerio de Relaciones Exteriores que fija la planta y fecha de iniciación de actividades de la Subsecretaría de Relaciones Económicas Internacionales y de la Dirección General de Promoción de Exportaciones; Resolución Exenta N°2 de 2019 de la Subsecretaría de Relaciones Económicas Internacionales que asigna funciones a las unidades de la Subsecretaría de Relaciones Económicas Internacionales; Resolución Exenta N° J-1 de 2019 de la Subsecretaría de Relaciones Económicas Internacionales, que delega la facultad de adoptar decisiones que en cada casos se indican; Resolución Exenta N° J-2 de 2019 de la Subsecretaría de Relaciones Económicas Internacionales, que delega la facultad de adoptar decisiones en materias de personal que en cada caso se indican.

Mision institucional

Contribuir al desarrollo económico del país mediante el diseño y ejecución de políticas orientadas a dirigir y fortalecer las relaciones económicas internacionales con el fin de consolidar la inserción de Chile en el mundo, a través de la negociación, administración e implementación de acuerdos económicos internacionales; y la activa participación de Chile en los foros y organismos internacionales que configuran las reglas del comercio internacional; promoviendo que los beneficios y oportunidades del libre comercio sean más inclusivos y favorezcan el bienestar para todos los habitantes del país.

Objetivos Estratégicos del Ministerio

Número	Descripción
5	Potenciar y promover la inserción de Chile en la economía mundial, negociando, profundizando y modernizando los tratados de libre comercio, participando activamente en instancias económicas multilaterales e impulsando un sistema global basado en reglas, con especial énfasis en el acercamiento con Asia Pacífico.
9	Modernizar las capacidades de nuestra Cancillería incorporando un pensamiento estratégico en sus áreas y relevando nuevas temáticas relacionadas con desafíos emergentes, estableciendo una gestión centrada en las personas.
10	Potenciar el trabajo con la sociedad civil y la inclusión de las regiones de Chile, de manera estratégica en materias de política exterior, permitiendo su proyección internacional, con especial énfasis en las zonas extremas del país, a través del impulso al desarrollo sostenible y el fortalecimiento de la presencia sub antártica y antártica.
11	Reconocer e incorporar en el quehacer del Ministerio de Relaciones Exteriores, las materias de género y diversidad de identidades, con énfasis en aprender de la experiencia de países avanzados en estas temáticas, para ponerlas al servicio del Estado de Chile.

Fuente: http://www.dipres.gob.cl/598/w3-propertyvalue-15219.html#instrumentos

AMENAZAS: MIS PRODUCTOS ESTRATÉGICOS

Nota: **https://www.dipres.gob.cl/597/articles-218122_doc_pdf.pdf**

Productos Estratégicos (Bienes y/o servicios)					
Número	Producto Estratégico	Descripción	Clientes	Aplica Gestión Territorial	Aplica Enfoque de Género
1	Políticas y planes relativos a la participación de Chile en las relaciones económicas internacionales a nivel bilateral, regional y multilateral.	Considera las acciones necesarias para el diseño, coordinación y ejecución de políticas y planes relativos a la participación de Chile en las relaciones económicas internacionales, conforme a las prioridades gubernamentales.	1,2,3,4,5,6,8	No	Si
2	Políticas de comercio exterior relativas al desarrollo de exportaciones y la promoción de la imagen de Chile en el exterior.	Incluye las acciones necesarias para el diseño de políticas y planes relativos al desarrollo de exportaciones y la promoción de la imagen de Chile en el exterior, conforme a las prioridades gubernamentales; e incluye la instrucción de la ejecución de dichas políticas y planes a la Dirección General de Promoción de Exportaciones.	1,2,3,4,5,6,8	No	Si
3	Acuerdos Económicos Internacionales.	Considera prospectar y proponer permanentemente la revisión y modernización de acuerdos económico comerciales, para generar iniciativas y ejes de convergencia que respondan a las nuevas dinámicas de la globalización. Asimismo, implica monitorear y gestionar la implementación y administración de mecanismos institucionales, adoptados por las partes, que garanticen el acceso a mercados, convocando a las contrapartes a realizar las reuniones establecidas y las que surjan en virtud de las necesidades comerciales, como, por ejemplo, las comisiones de libre comercio, las comisiones administradoras, los comités sectoriales, entre otros mecanismos. Involucra desarrollar estrategias e instrumentos de política comercial para consolidar la inserción económico comercial de Chile en el exterior, entre otras, en cadenas	1,2,3,4,5,6,7,8,9	No	Si

AMENAZAS: MIS PRODUCTOS ESTRATÉGICOS

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

LA CIBERSEGURIDAD
DEBE ESTAR ALINEADA CON EL NEGOCIO

AMENAZAS: ¿QUE PUEDEN AFECTAR?

Que le puede suceder a mis activos o a los de la institución:

Confidencialidad: Se puede comprometer la confidencialidad y, en consecuencia, datos sensibles pueden llegar a ser conocidos por terceras partes no autorizadas. A veces esto se utiliza para extorsionar a las personas o las instituciones. Existe la Ley N°20.285, pero …

Integridad: Se pueden ver adulterados, modificados, dañados, eliminados nuestros activos. A veces esto se hace con el objetivo de afectar la imagen de la institución o generar desinformación por ejemplo.

Disponibilidad: Pueden llegar a estar no disponibles, por múltiples razones, tales como: DDoS, encriptación (ransomware), falla en los medios físicos que los almacenan, etc.

- **Recuerde: CID**

AMENAZAS: ¿QUE PUEDEN AFECTAR?

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Es importante entender como pueden verse afectado nuestro activo respecto de la tríada CID

Para evaluar los riesgos y planes de mitigación de los posibles amenazas, se necesita información acerca del activo.

Un elemento clave es determinar qué valor le asigna la organización a la disponibilidad, integridad y confidencialidad (tríada CID) de cada activo, proceso o producto estratégico.

Cada uno de los activos evaluados requerirá distintos niveles de protección, dependiendo de la función que desempeñe y el valor de la tríada CID para dicha función.

http://www.dipres.gob.cl/598/articles-51683_intro_instrumentos_2016_18_05.xlsx

AMENAZAS: ¿QUE PUEDEN AFECTAR?

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Es importante entender el valor de las señales de datos (tríada CID)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	*Nombre de la Institución:*														
2	CARACTERIZACIÓN DEL ACTIVO						IDENTIFICACIÓN Y CARACTERIZACION DE LOS RIESGOS						MEDIDAS DE MITIGACION		
3	Proceso	Nombre Activo	Confidencialidad	Integridad	Disponibilidad	Criticidad	Amenaza	Vulnerabilidad (Debilidad)	Descripción del Riesgo	Probabilidad de ocurrencia	Impacto	Severidad	Control para mitigar el riesgo	Cumplimiento	Nombre del producto esperado
4															
5															
6															
7															
8															
9															
10															
11															
12															

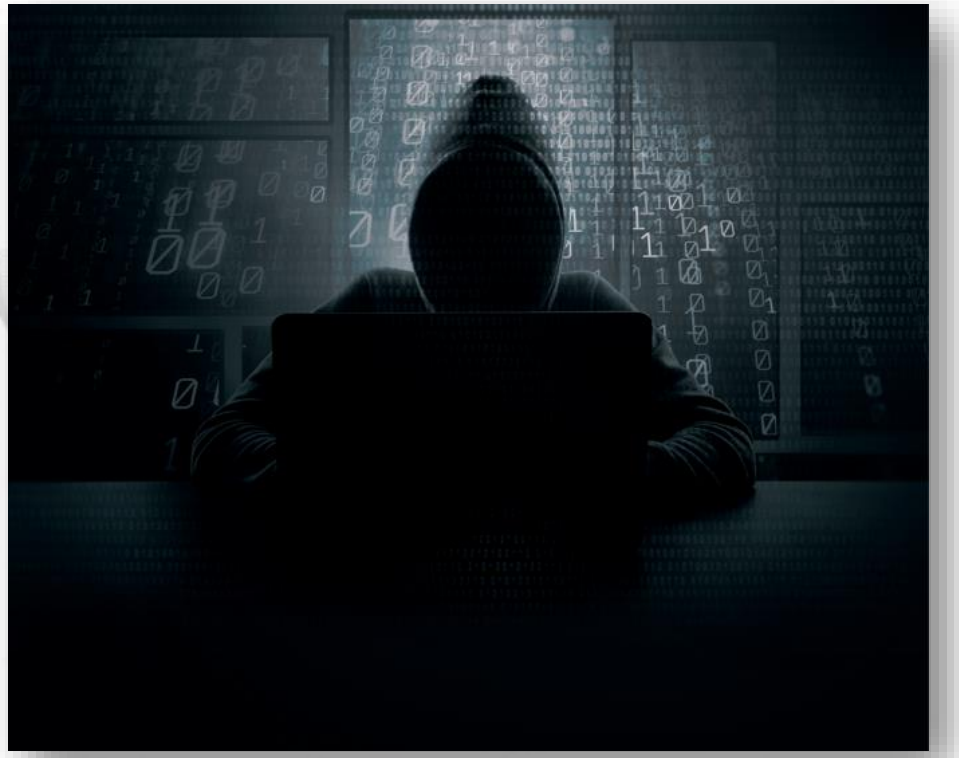
http://www.dipres.gob.cl/598/articles-51683_intro_instrumentos_2016_18_05.xlsx

AMENAZAS: ¿QUE PUEDEN AFECTAR?

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Es importante entender claramente el valor la tríada CID:

Disponibilidad – Acceso confiable y oportuno a datos y recursos. Dispositivos de red, computadoras, PLC, HMI y otros, que brinden una funcionalidad adecuada para tener un desempeño predecible y aceptable.



AMENAZAS: ¿QUE PUEDEN AFECTAR?

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Es importante entender claramente el valor la tríada CID:

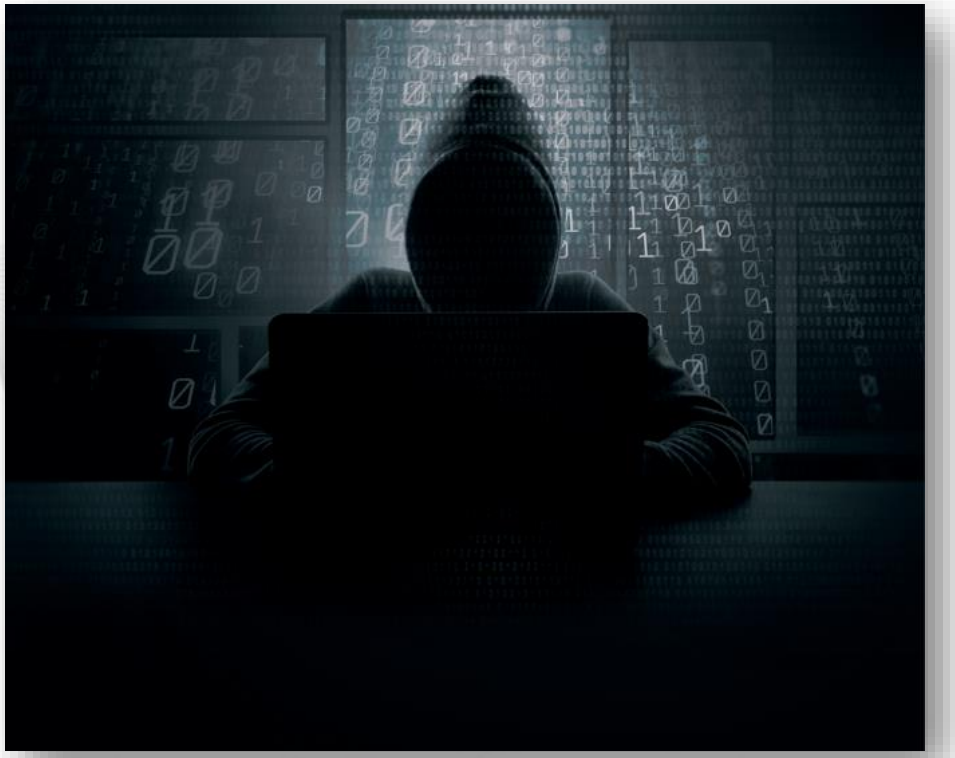
Integridad – Se brinda precisión y confiabilidad de la información y de los sistemas, y se previene cualquier modificación no autorizada. El hardware, software y los mecanismos de comunicación deben funcionar conjuntamente para mantener y procesar datos correctamente y trasladar datos a los destinos previstos, sin alteraciones inesperadas.

AMENAZAS: ¿QUE PUEDEN AFECTAR?

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Es importante entender el valor de las señales de datos (tríada CID)

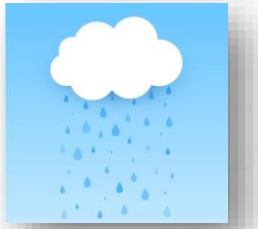
Confidencialidad – Se establece el nivel necesario de secreto y se previene la divulgación no autorizada. La idea es prevenir la divulgación no autorizada de información.

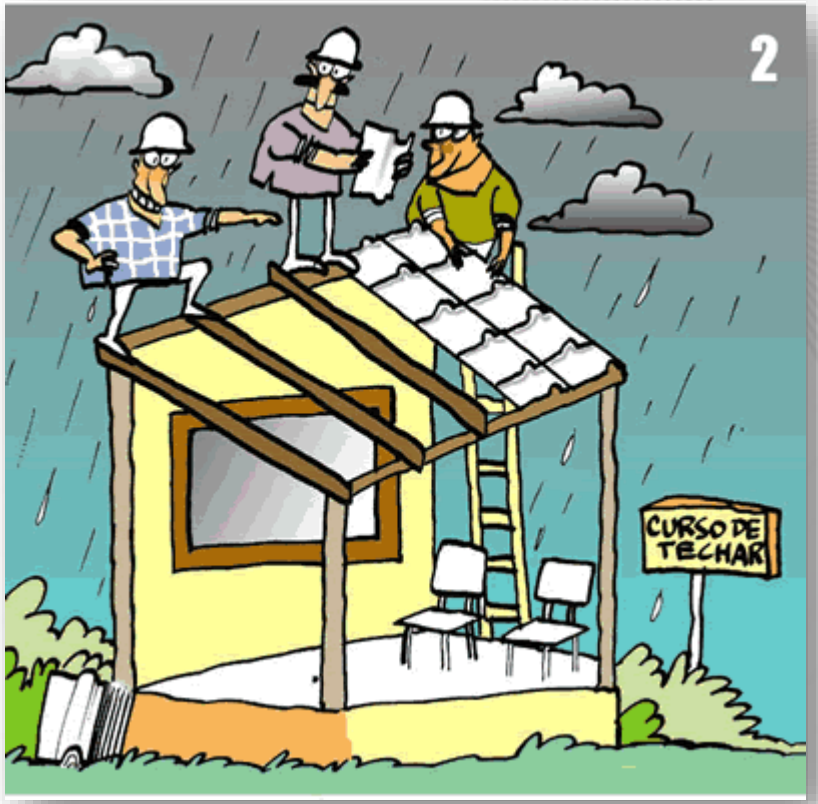


AMENAZAS: ¿QUE PUEDEN AFECTAR?

Una vulnerabilidad es una debilidad de un activo o control que puede ser aprovechada por una amenaza

AMENAZA = LLUVIA



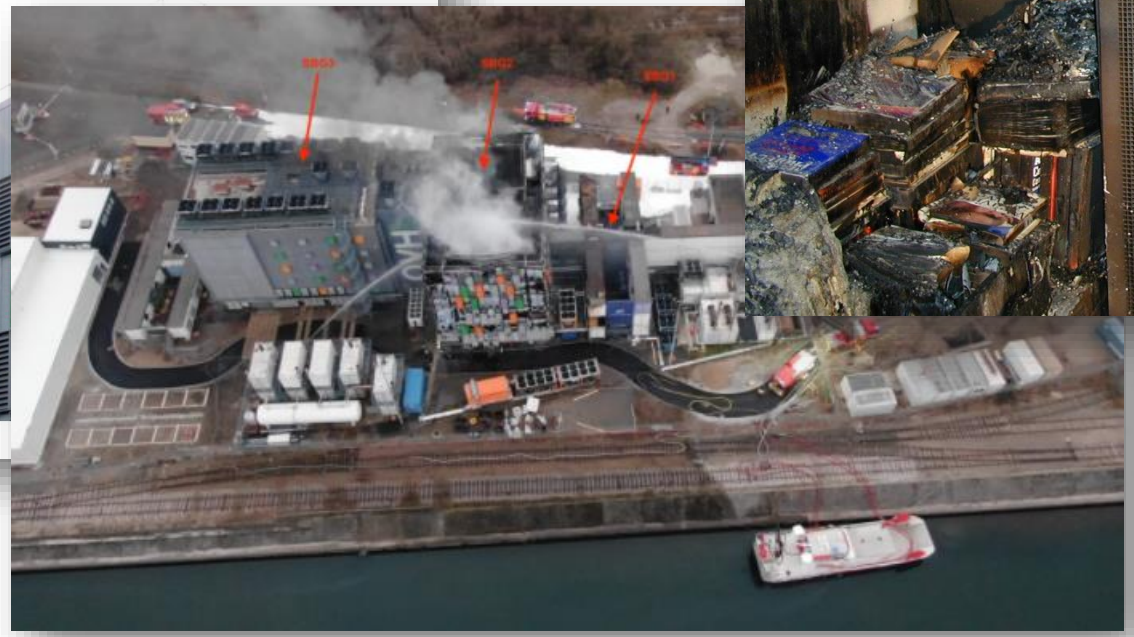


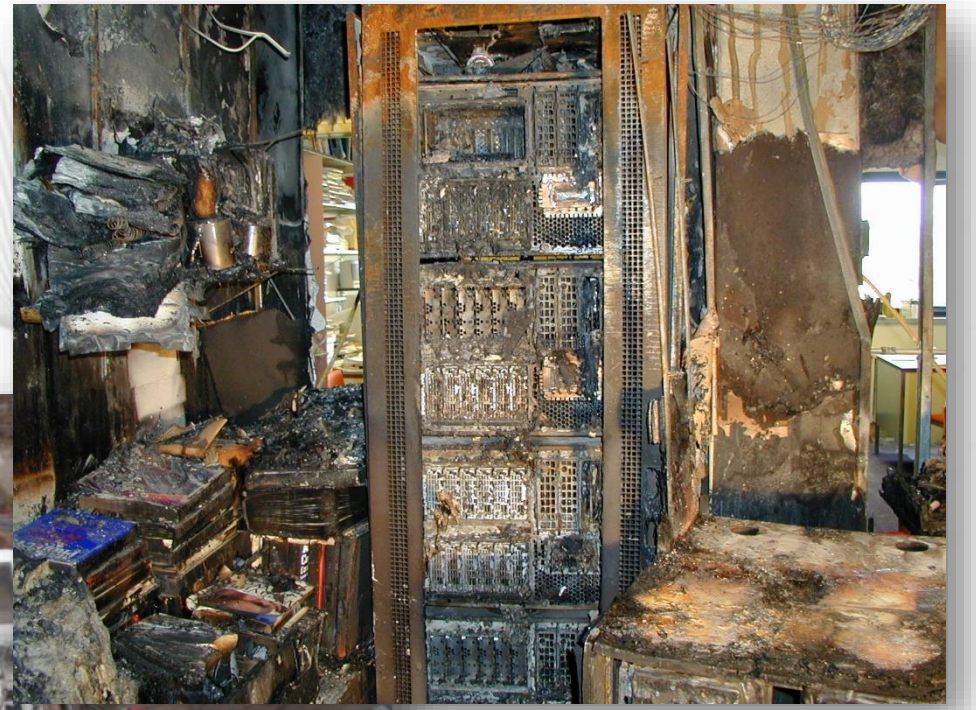
ACTIVO = MI CASA

VULNERABILIDAD =
FALTA DE TECHO

EJEMPLOS DE AMENAZAS

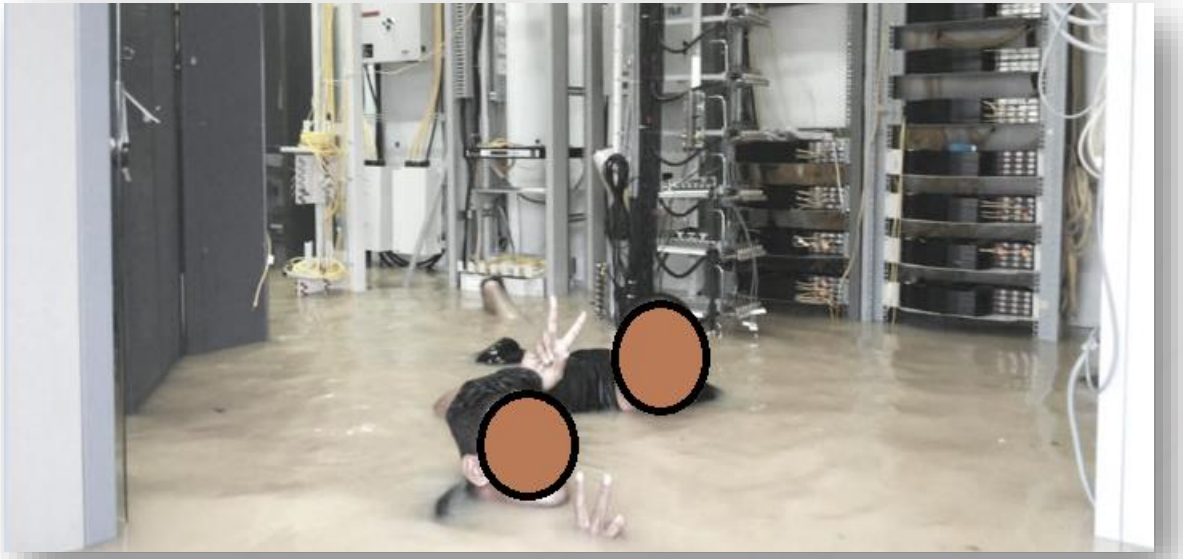
- **Daño físico:** Fuego, agua/lluvia, destrucción de equipos o medios, Polvo, corrosión, congelamiento.

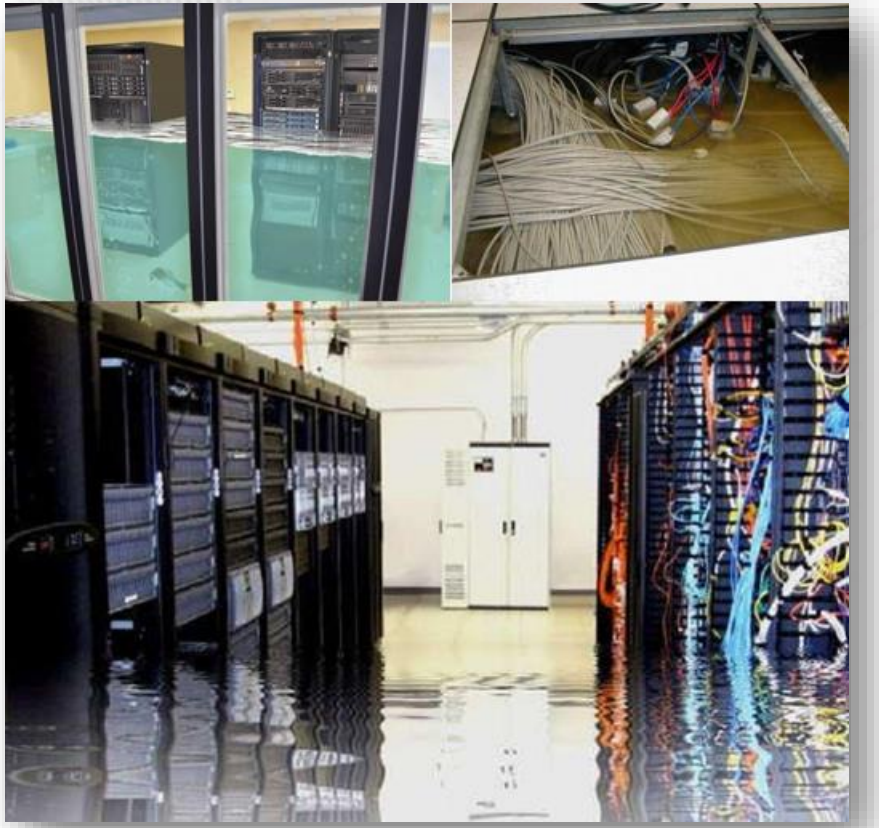




EJEMPLOS DE AMENAZAS

- **Eventos naturales:** Fenómeno climático, fenómeno sísmico, fenómeno volcánico, fenómeno meteorológico, inundación.





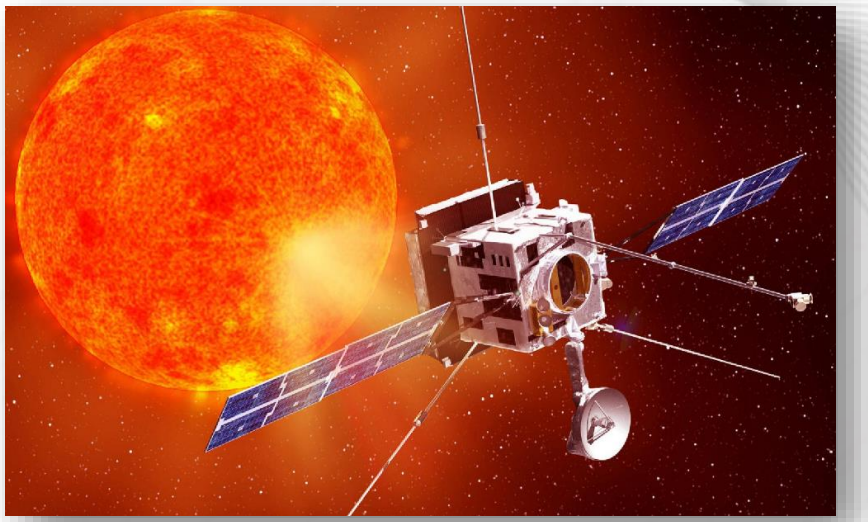
EJEMPLOS DE AMENAZAS

- **Pérdida de servicios esenciales:** Falla de aire acondicionado o suministro de agua, pérdida de suministro de energía, falla de equipamiento de telecomunicaciones.

EJEMPLOS DE AMENAZAS

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Perturbación debido a radiación: Radiación electromagnética, radiación térmica, pulsos electromagnéticos .



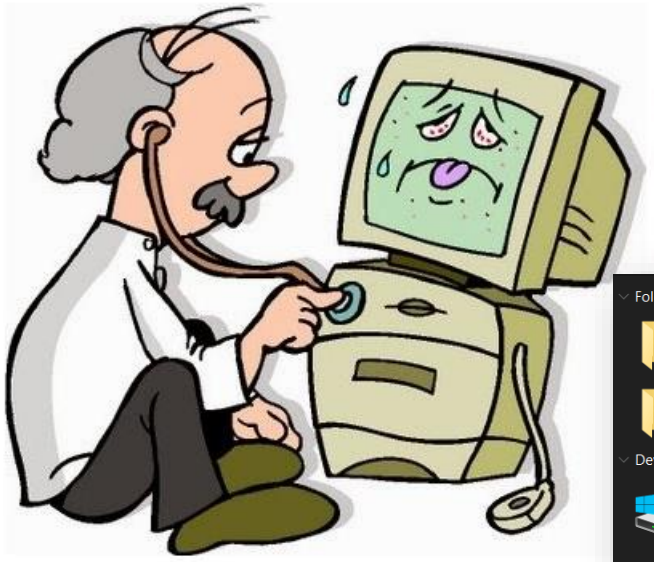
EJEMPLOS DE AMENAZAS

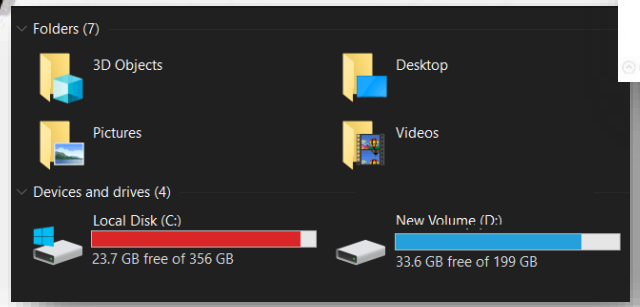
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

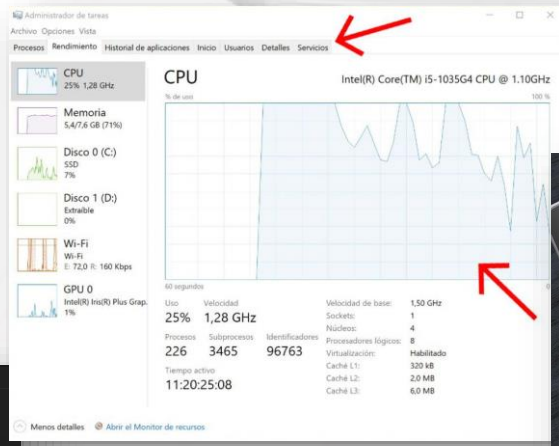
Compromiso de información: Señales de interferencia e interceptación que comprometen activos de información, espionaje remoto, escucha secreta, robo de medios o documentos, robo de equipos, recuperación de medios reciclados o descartados, divulgación o exfiltración, datos de fuentes poco fiables, manipulación con hardware, manipulación con software.

EJEMPLOS DE AMENAZAS

- **Fallas técnicas:** Falla de equipo, mal funcionamiento del equipo, saturación del sistema de información, mal funcionamiento del software, brecha de mantenimiento del sistema de información.



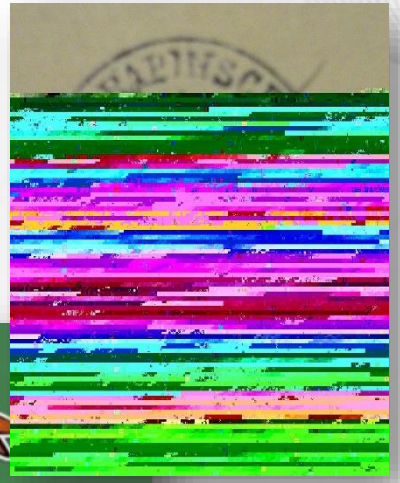




EJEMPLOS DE AMENAZAS

- **Acciones no autorizadas:** Uso no autorizado del equipo, copia fraudulenta de software, uso de software falsificado o copiado, corrupción de datos, procesamiento ilegal de datos.

Acceso no autorizado



Corrupción de datos

Uso de software sin licencia

Procesamiento ilegal de datos

EJEMPLOS DE AMENAZAS

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Compromiso de funciones: Error de uso, abuso de derechos, falsificación de derechos, negación de acciones, brecha de disponibilidad de personal.

Pueden existir otras fuentes de amenazas de las siguientes vertientes a analizar según el caso:

i. Crackers.
ii. Delitos informáticos.
iii. Terrorismo.
iv. Espionaje industrial (nacional o transnacional).
v. Internos.

EJEMPLOS DE VULNERABILIDADES

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Tipo Hardware:

- Falta de mantención en los equipos de almacenamiento.
- Un almacenamiento de datos desprotegido.
- Un sistema de copias sin control.

Tipo Software:

- Un software si suficiente testing.
- No desconectarse o bloquear la sesión.
- Una interfaz de usuario complicada → Induce error de uso

EJEMPLOS DE VULNERABILIDADES

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Tipo Red:

- Transferencias de contraseñas en claro (HTTP).
- Débil protección de los cables.

Tipo Personal:

- Falta de personal.
- Procedimientos inadecuados de reclutamiento.
- ¡Falta de entrenamiento en seguridad!
- ¡Falta de concientización en seguridad!

EJEMPLOS DE VULNERABILIDADES

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Tipo Site:

- Ubicación de las instalaciones en un área susceptible de inundación: Cota 30 por ejemplo (*).
- Una Red de Energía inestable.
- Falta de registros o logs de las actividades de operadores y administradores.

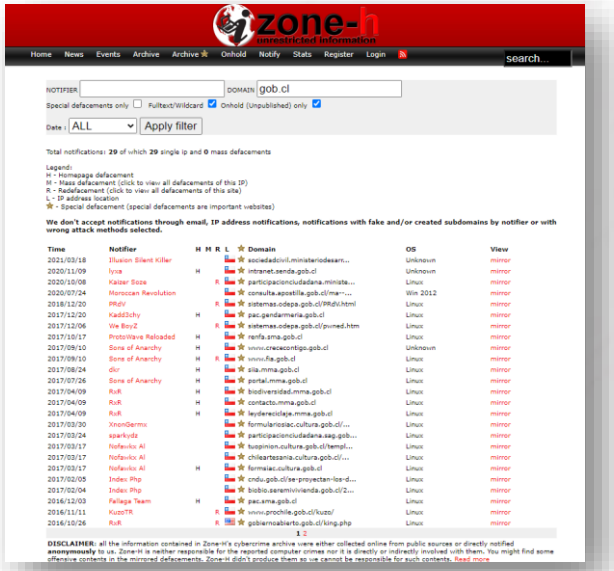
* https://senapred.cl/evacuacion-por-tsunami/

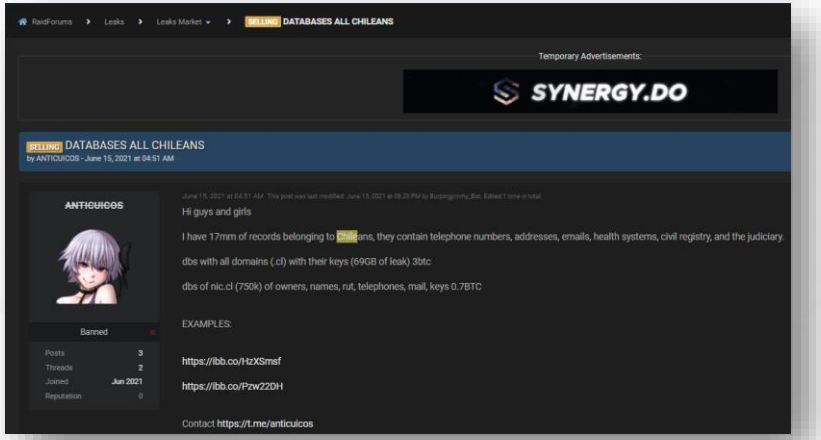
¿CUÁNTO TIEMPO DEMORA EN SER DETECTADO UN CIBERATAQUE?

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Las cifras son diversas, dependiendo del tipo de ataque, el objetivo y el tipo de activo comprometido. Poe ejemplos:

- Minutos ante una denegación de servicios.
- Horas en un defacement de sitio web.
- Meses en algunos tipos de exfiltración de datos.
- Años o décadas en infiltraciones de alto nivel.





OTRO CONCEPTO: RIESGO

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Los riesgos cibernéticos son una función de:

- Las consecuencias o impactos de un ataque exitoso contra un activo; y
- La probabilidad de éxito del ataque a un activo.

La probabilidad es una función de:

- El atractivo que tenga el activo para el adversario;
- La magnitud de la amenaza que represente el adversario; y
- El grado de vulnerabilidad o susceptibilidad del activo a verse vulnerado por un adversario.

OTRO CONCEPTO: SEVERIDAD DEL RIESGO

- SEVERIDAD DEL RIESGO = P x I
- P= Probabilidad de que una amenaza explote una vulnerabilidad
- I= Impacto que se produce si se materializa que la amenaza explote la vulnerabilidad

PROBABILIDAD

Categoría	Valor	Descripción
Casi certeza	5	Riesgo cuya probabilidad de ocurrencia es muy alta, es decir, se tiene un alto grado de seguridad que éste se presente en el año en curso. (90% a 100%).
Probable	4	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre 66% a 89% de seguridad que éste se presente en el año en curso.
Moderado	3	Riesgo cuya probabilidad de ocurrencia es media, es decir, se tiene entre 31% a 65% de seguridad que éste se presente en el año en curso.
Improbable	2	Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene entre 11% a 30% de seguridad que éste se presente en el año en curso.
Muy improbable	1	Riesgo cuya probabilidad de ocurrencia es muy baja, es decir, se tiene entre 1% a 10% de seguridad que éste se presente en el año en curso.

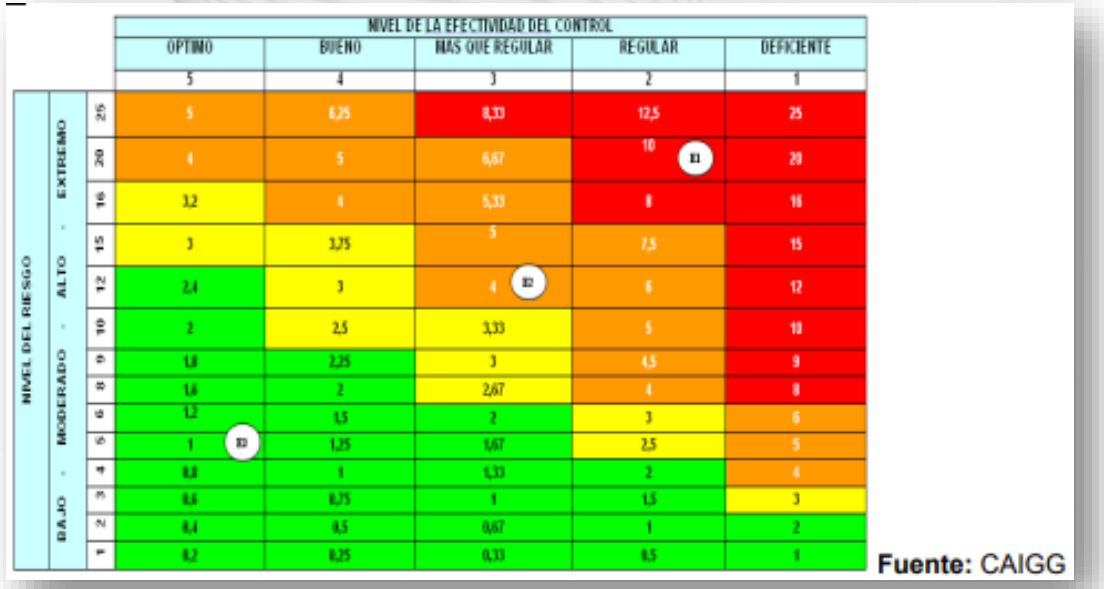
IMPACTO

Categoría	Valor	Descripción
Catastróficas	5	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto catastrófico en el presupuesto y/o comprometen totalmente la imagen pública de la organización y del Gobierno. Su materialización dañaría gravemente el desarrollo del proceso y el cumplimiento de los objetivos, impidiendo finalmente que estos se logren en el año en curso.
Mayores	4	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto importante en el presupuesto y/o comprometen fuertemente la imagen pública de la organización y del Gobierno. Su materialización dañaría significativamente el desarrollo del proceso y el cumplimiento de los objetivos, impidiendo que se desarrollen total o parcialmente en forma normal en el año en curso.
Moderadas	3	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto moderado en el presupuesto y/o comprometen moderadamente la imagen pública de la organización y del Gobierno. Su materialización causaría un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle parcialmente en forma normal en el año en curso.
Menores	2	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto menor en el presupuesto y/o comprometen de forma menor la imagen pública de la organización y del Gobierno. Su materialización causaría un bajo daño en el desarrollo del proceso y no afectaría el cumplimiento de los objetivos en el año en curso.
Insignificantes	1	Riesgo cuya materialización no genera pérdidas financieras ($) ni compromete de ninguna forma la imagen pública de la organización y del Gobierno. Su materialización puede tener un pequeño o nulo efecto en el desarrollo del proceso y que no afectaría el cumplimiento de los objetivos en el año en curso.

RIESGO

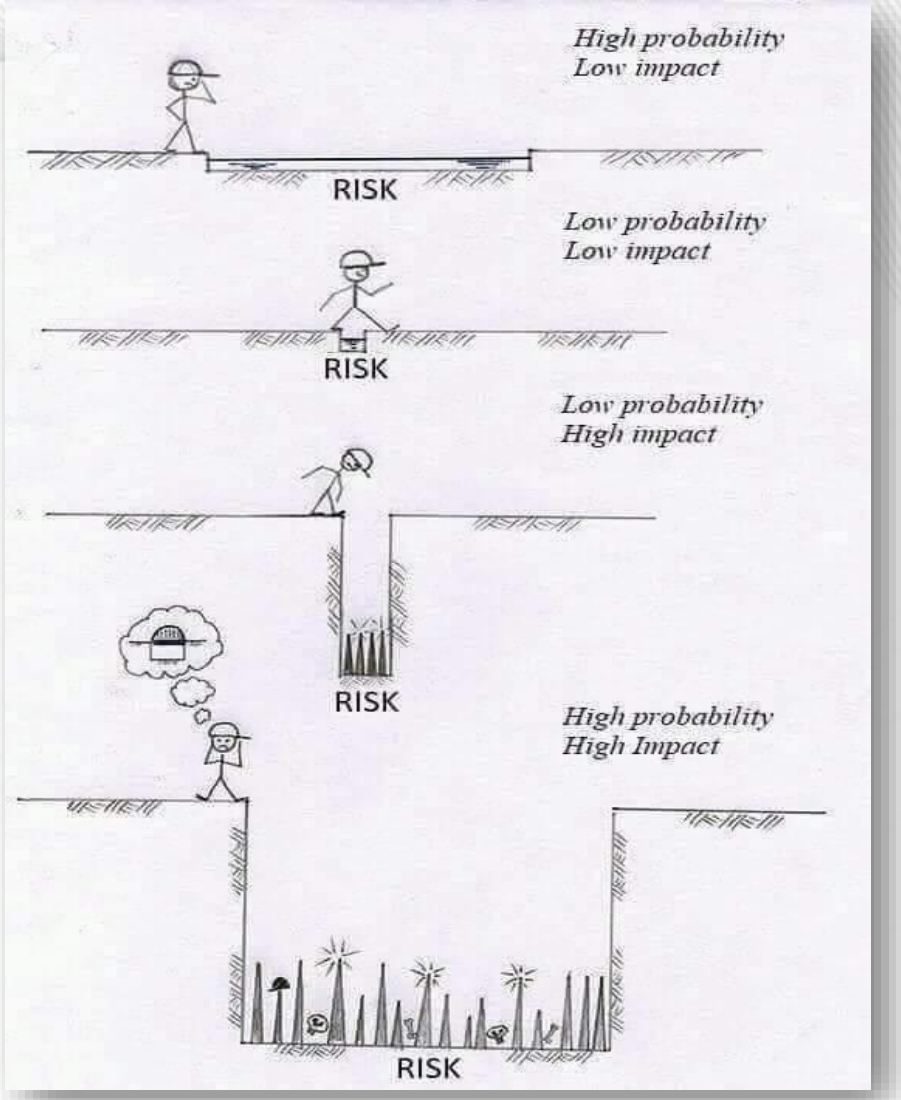
Con esto se obtiene una tabla de severidad de riesgos que permite gestionarlos, y de esa manera administrar los riesgos más altos para nuestros activos relevantes. **[Recuerde: los recursos en general son escasos y hay que asignarlos con criterios de priorización]**

NIVEL PROBABILIDAD (P)	NIVEL IMPACTO (I)	SEVERIDAD DEL RIESGO S = (P x I)
Casi Certeza (5)	Catastróficas (5)	EXTREMO (25)
Casi Certeza (5)	Mayores (4)	EXTREMO (20)
Casi Certeza (5)	Moderadas (3)	EXTREMO (15)
Casi Certeza (5)	Menores (2)	ALTO (10)
Casi Certeza (5)	Insignificantes (1)	ALTO (5)
Probable (4)	Catastróficas (5)	EXTREMO (20)
Probable (4)	Mayores (4)	EXTREMO (16)
Probable (4)	Moderadas (3)	ALTO (12)
Probable (4)	Menores (2)	ALTO (8)
Probable (4)	Insignificantes (1)	MODERADO (4)
Moderado (3)	Catastróficas (5)	EXTREMO (15)
Moderado (3)	Mayores (4)	EXTREMO (12)
Moderado (3)	Moderadas (3)	ALTO (9)
Moderado (3)	Menores (2)	MODERADO (6)
Moderado (3)	Insignificantes (1)	BAJO (3)
Improbable (2)	Catastróficas (5)	EXTREMO (10)
Improbable (2)	Mayores (4)	ALTO (8)
Improbable (2)	Moderadas (3)	MODERADO (6)
Improbable (2)	Menores (2)	BAJO (4)
Improbable (2)	Insignificantes (1)	BAJO (2)
muy improbable (1)	Catastróficas (5)	ALTO (5)
muy improbable (1)	Mayores (4)	ALTO (4)
muy improbable (1)	Moderadas (3)	MODERADO (3)
muy improbable (1)	Menores (2)	BAJO (2)
muy improbable (1)	Insignificantes (1)	BAJO (1)



Fuente: CAIGG

RIESGO: AFIANCEMOS EL CONCEPTO DE RIESGO



SEVERIDAD ALTO (5)
Casi Certeza x Insignificantes

SEVERIDAD BAJO (1)
Muy improbable x Insignificantes

SEVERIDAD ALTO (5)
Muy Improbable x Catastróficas

SEVERIDAD EXTREMO (25)
Casi certeza x Catastróficas

RIESGO: AFIANCEMOS EL CONCEPTO DE RIESGO

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Evaluación de Riesgos: Proceso que analiza los niveles de riesgo en un sistema, calculados con base en:

- El valor de los activos
- Las amenazas a todos los activos
- Las vulnerabilidades en los activos y la probabilidad de que sean aprovechadas por las amenazas

Gestión de riesgos – Sistema que emplea datos de la evaluación de riesgos para identificar, seleccionar y adoptar medidas de seguridad justificadas según:

- El riesgo identificado para los activos
- Los controles seleccionados para reducir los riesgos a niveles aceptables
- La estimación de riesgos residuales

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	*Nombre de la Institución:*														
2	CARACTERIZACIÓN DEL ACTIVO						IDENTIFICACIÓN Y CARACTERIZACION DE LOS RIESGOS						MEDIDAS DE MITIGACION		
3	Proceso	Nombre Activo	Confidencialidad	Integridad	Disponibilidad	Criticidad	Amenaza	Vulnerabilidad (Debilidad)	Descripción del Riesgo	Probabilidad de ocurrencia	Impacto	Severidad	Control para mitigar el riesgo	Cumplimiento	Nombre del producto esperado
4															
5															
6															
7															
8															
9															
10															
11															
12															

RIESGO: AFIANCEMOS EL CONCEPTO DE RIESGO

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Enfoque de 5 pasos para el proceso de gestión de riesgos:

1. Caracterización de activos

- Identificar los activos críticos, funciones, infraestructuras, interdependencias, etc. • Evaluar el impacto si los activos son interrumpidos o vulnerados.

2. Evaluación de amenazas

- Identificar y caracterizar los agentes de amenaza.
- Evaluar cuán atractivos son los blancos para el agente de amenaza.

3. Análisis de vulnerabilidades

- Identificar vulnerabilidades y susceptibilidades a nivel del sistema y de los componentes, y calcular el grado de vulnerabilidad.
- Determinar la eficacia de las contramedidas existentes.

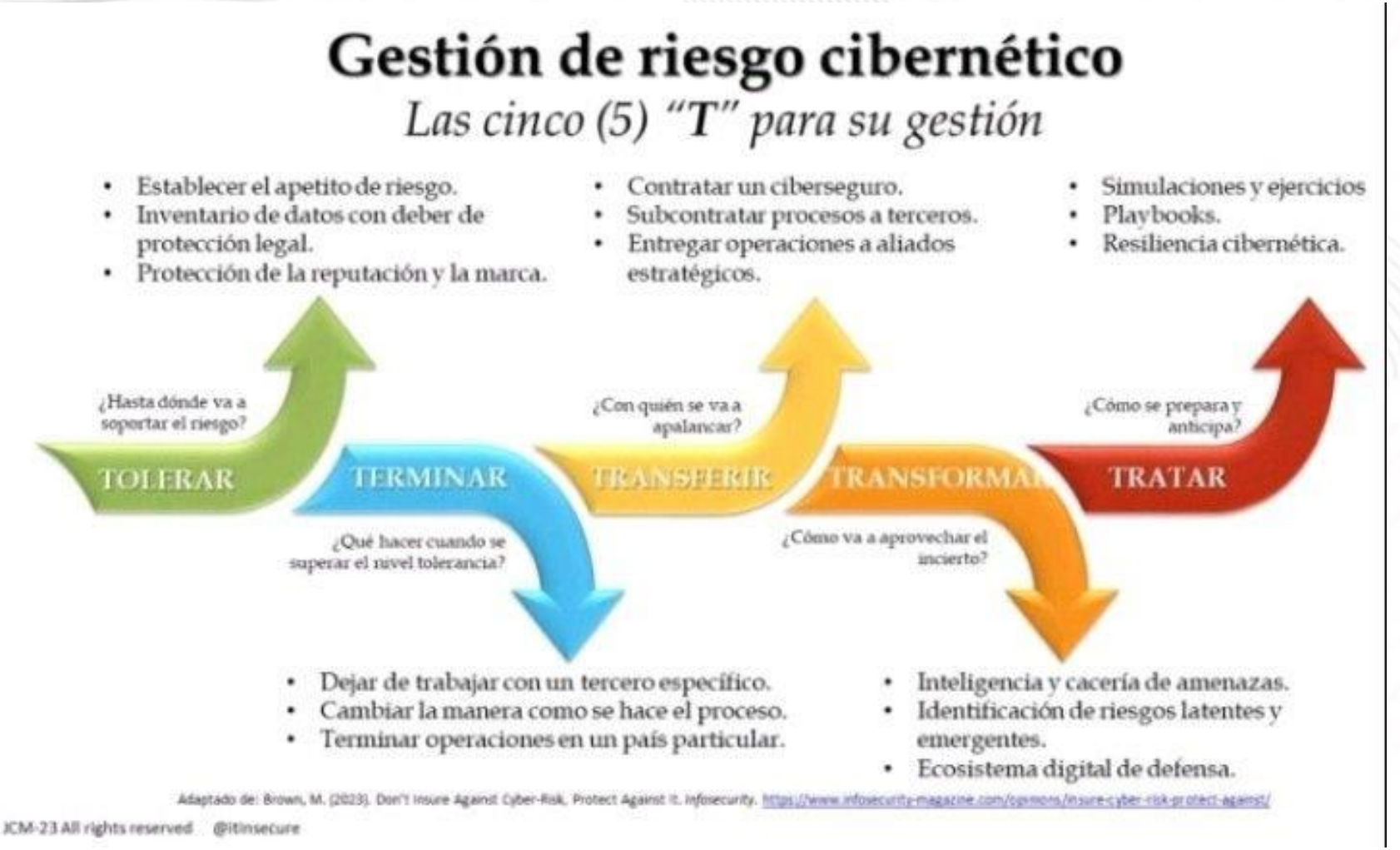
4. Evaluación y priorización de riesgos

- Calcular el riesgo de sufrir un ataque exitoso y priorizar todas las exposiciones a riesgos.

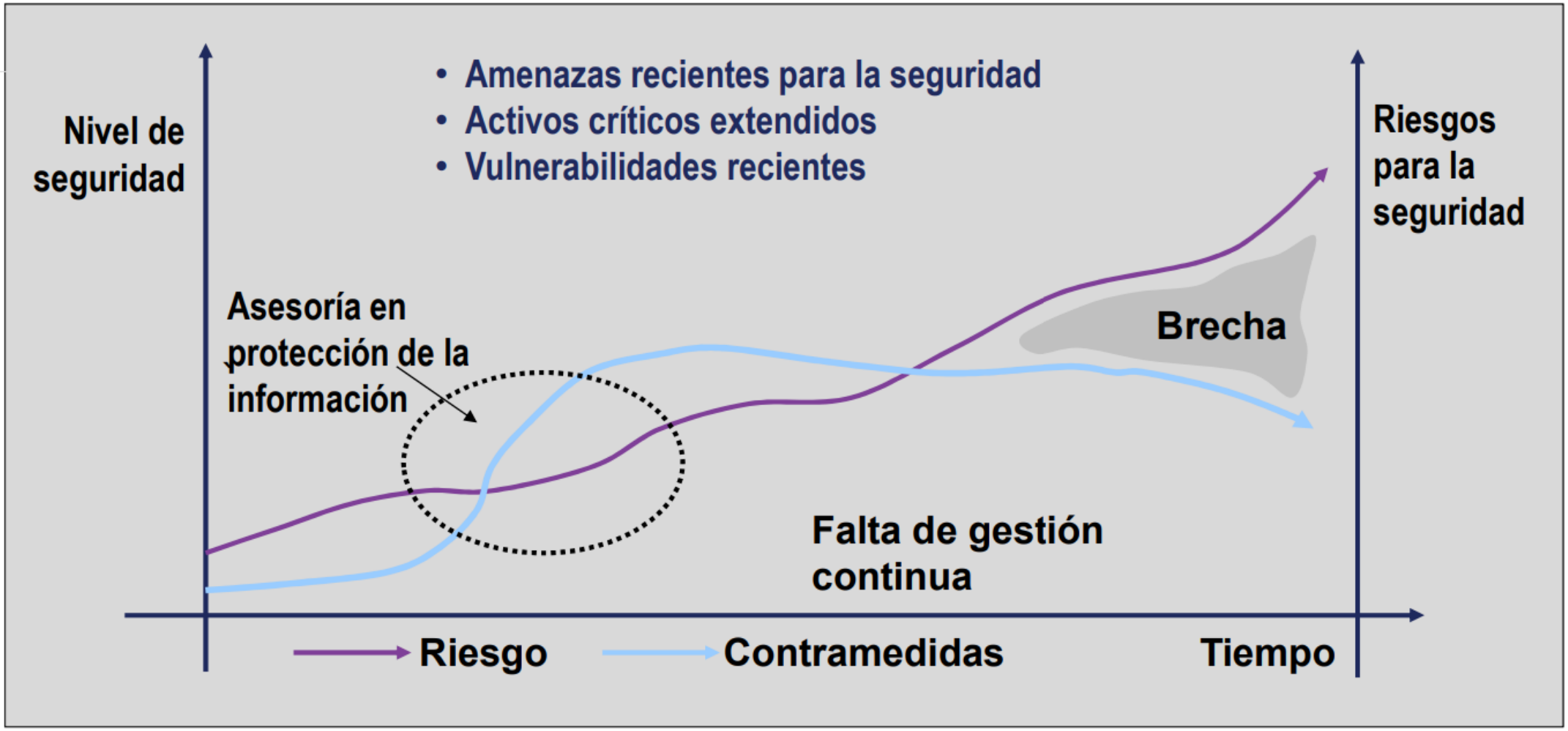
5. Mitigación de riesgos y sostenibilidad

- Identificar y evaluar posibles contramedidas.
- Priorizar posibles mejoras.

RIESGO: AFIANCEMOS EL CONCEPTO DE RIESGO



RIESGO: AFIANCEMOS EL CONCEPTO DE RIESGO



CÓDIGO MALICIOSO

- En un mundo interconectado, la información y los procesos, sistemas y redes relacionados constituyen activos empresariales/institucionales críticos.

- Las organizaciones y sus sistemas y redes de información se enfrentan a amenazas de seguridad procedentes de una amplia gama de fuentes, como el fraude informático, el espionaje, el sabotaje, el vandalismo, los incendios y las inundaciones.

- Los daños a los sistemas y redes de información pueden ser causados por códigos maliciosos, la piratería informática y los ataques de denegación de servicio se han vuelto más comunes, más ambiciosos y cada vez más sofisticados.

¿QUÉ ES EL CÓDIGO MALICIOSO O MALWARE?

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Son programas que tienen como objetivo acceder a su sistema sin que, en general, se detecte su presencia.

En función de la intención u objetivo del Cracker, el programa podría:

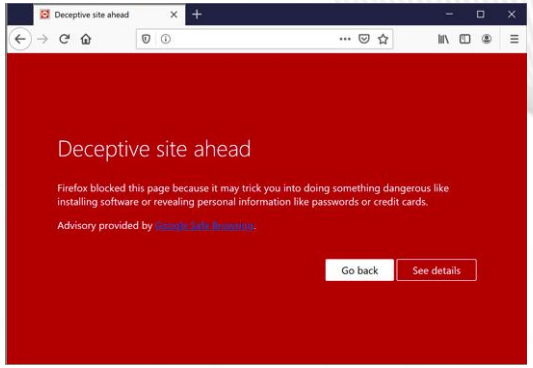
- Robar credenciales, datos bancarios, información o cualquier activo de información.
- Crear redes botnet con los computadores institucionales o personales, y hacerlos participes de acciones delictivas.
- Utilización no autorizada de los recursos computacionales (CPU/RAM/DISCO).
- Destruir o inutilizar un sistema de tratamiento de información o sus partes o componentes, o impedir, obstaculizar o modificar su funcionamiento.
- Usar o conocer indebidamente la información contenida en un sistema de tratamiento de la misma, interceptarla, interferirla o acceder a él.
- Alterar, dañar o destruir los datos contenidos en un sistema de tratamiento de información.
- Revelar o difundir los datos contenidos en un sistema de información.
- Cifrar del contenido. Con esto se intenta que los usuarios paguen un rescate por sus datos.

Nota: Revise más información en CSIRT de Gobierno:
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-evitar-malware/

¿CUÁLES SON LOS TIPOS DE CÓDIGO MALICIOSO MÁS COMUNES?

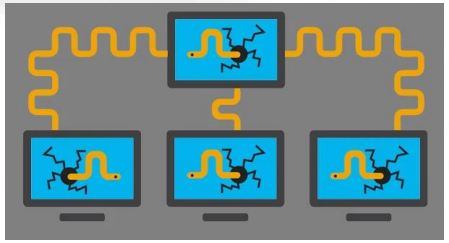
- Virus

Tiene como objetivo alterar el funcionamiento de los equipos infectados, su modo de actuar es mediante la ejecución del código, alojarse en la memoria RAM. Por lo que son realmente dañinos a la hora de consumir recursos de nuestro equipo, provocando una pérdida de productividad o daños a nuestros datos.



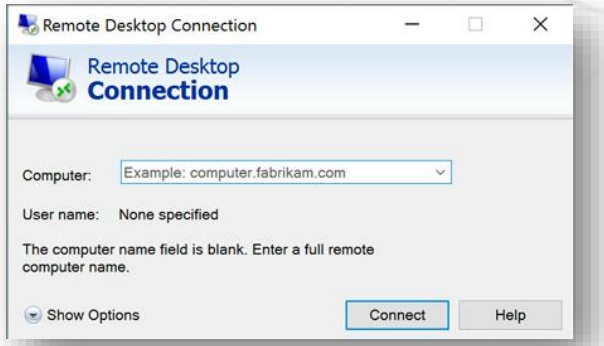
URL maliciosa

pendrive



Movimiento lateral

RDP

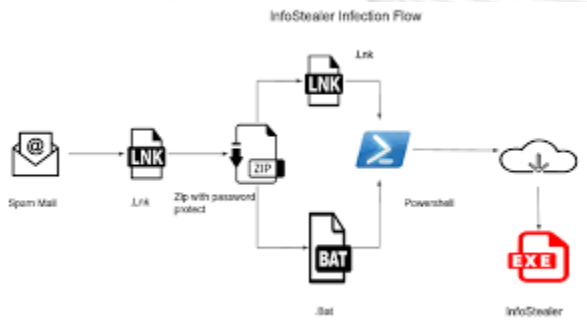


Email

¿CUÁLES SON LOS TIPOS DE CÓDIGO MALICIOSO MÁS COMUNES?

Un infostealer (también conocido como "stealer" o "credential stealer")

- es un tipo específico de malware cuya función principal es robar información sensible almacenada en un dispositivo o en aplicaciones específicas. Los infostealers suelen enfocarse en obtener datos como nombres de usuario, contraseñas, números de tarjetas de crédito u otra información personal o financiera valiosa. Estos datos robados luego pueden ser utilizados por los atacantes para cometer fraudes, robo de identidad u otros delitos cibernéticos.



Zeus (Zbot)
SpyEye
TrickBot
Ursnif (Gozi)
Pony
FormBook
AZORult
Agent Tesla
RedLine

¿CUÁLES SON LOS TIPOS DE CÓDIGO MALICIOSO MÁS COMUNES?

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Un infostealer (también conocido como "stealer" o "credential stealer")

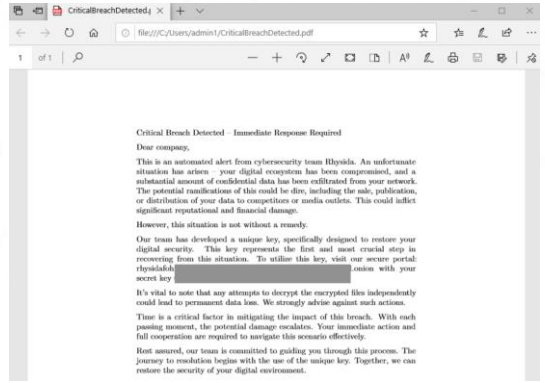
- Zeus: También conocido como Zbot, es uno de los infostealers más notorios. Está diseñado para robar información bancaria, como credenciales de inicio de sesión y detalles de tarjetas de crédito.
- SpyEye: Similar a Zeus, SpyEye es otro infostealer que se enfoca en el robo de información financiera, especialmente relacionada con transacciones bancarias en línea.
- TrickBot: Inicialmente un troyano bancario, TrickBot se ha convertido en una amenaza multifuncional que incluye capacidades de robo de información. Puede robar credenciales, datos personales y realizar ataques de suplantación de identidad.
- Ursnif: Conocido también como Gozi, Ursnif es un infostealer que se dirige principalmente a usuarios de Windows y está diseñado para robar información confidencial, como datos bancarios y credenciales de inicio de sesión.
- Pony: Este infostealer se distribuye a través de campañas de spam y se enfoca en el robo de información personal y financiera, como contraseñas almacenadas en navegadores y clientes de correo electrónico.

¿CUÁLES SON LOS TIPOS DE CÓDIGO MALICIOSO MÁS COMUNES?

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Ransomware

- Malware que toma por completo el control de los datos de un dispositivo, cifrando la información del usuario para, a continuación, pedir dinero a cambio de liberar o descifrar los ficheros del dispositivo. También aumentan la presión sobre la víctima robando los datos y amenazando con liberar en internet.
- Es importante destacar que pagar el rescate **no garantiza** necesariamente la recuperación de los archivos y, además, fomenta la continuidad de estas prácticas delictivas.
- La mejor manera de protegerse contra el ransomware es mantener actualizado el software, utilizar soluciones de seguridad confiables, hacer copias de seguridad periódicas de los archivos y tener precaución al abrir correos electrónicos y descargar archivos de fuentes desconocidas o no confiables.

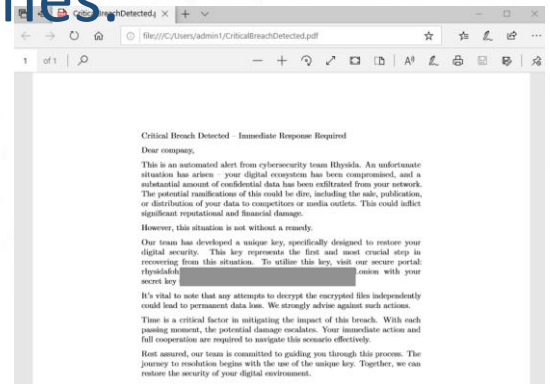


¿CUÁLES SON LOS TIPOS DE CÓDIGO MALICIOSO MÁS COMUNES?

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Ransomware: Algunos vectores de entrada.

- Phishing/Spearphishing.
- Remote Desktop Protocol. (ataques de fuerza bruta)
- Explotación de vulnerabilidades.
- Compra de credenciales de acceso.
- Comprometer a terceras partes (proveedores por ejemplo).
- Reclutar a personal interno de las empresas o instituciones.



¿QUÉ ESTÁ HACIENDO NUESTRO ENCARGADO DE CIBERSEGURIDAD?

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

a) establecer una política formal que prohíbe el uso de software no autorizado;

b) implementar controles que evitan o detectan el uso de software no autorizado (es decir, la creación de una lista blanca de aplicaciones);

c) implementar controles que eviten o detecten el uso de sitios web desconocidos o que se sospecha son maliciosos (es decir, la elaboración de una lista negra).

d) establecimiento de una política formal para protegerse contra los riesgos asociados al obtener archivos y software ya sea de redes externas o a través de cualquier otro medio, indicando las medidas de protección que se deberían tomar;

e) reducción de las vulnerabilidades que se podrían desencadenar por el malware, es decir, a través de la administración de vulnerabilidades técnicas;

¿QUÉ ESTÁ HACIENDO NUESTRO ENCARGADO DE CIBERSEGURIDAD?

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

f) realizar revisiones periódicas del software y del contenido de los datos de los sistemas que apoyan los procesos críticos del negocio; se debería investigar formalmente la presencia de cualquier tipo de archivos o modificaciones no autorizados;

g) instalación y actualización periódica de software de detección de malware y reparación para analizar computadores y medios como control de precaución o, de manera rutinaria; el análisis debería incluir:

- analizar solo los archivos recibidos a través de redes o mediante cualquier forma de medios de almacenamiento, en busca de malware antes de su uso;
- analizar datos adjuntos de correos electrónicos en busca de malware antes de su uso; este análisis se debería realizar en diferentes lugares, es decir, en servidores de correo electrónico, computadores de escritorio y al ingresar a la red de la organización;
- analizar páginas web en busca de malware;

¿QUÉ ESTÁ HACIENDO NUESTRO ENCARGADO DE CIBERSEGURIDAD?

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

h) definir procedimientos y responsabilidades que involucren la protección contra malware en los sistemas,

i) preparar planes de continuidad adecuados para recuperarse contra ataques de malware, incluidos todos los datos, respaldo de software y disposiciones de recuperación necesarios;

j) implementar procedimientos para recopilar información de manera regular, como la suscripción a listas de correo electrónico o verificar los sitios web que brindan información sobre el nuevo malware;

k) implementar procedimientos para verificar la información relacionada al malware y asegurarse de que los boletines de advertencia son precisos e informativos; los gerentes se deberían asegurar de que se utilicen fuentes calificadas, es decir, publicaciones de reconocido prestigio, sitios de internet o proveedores productores de software de protección contra malware confiables para diferenciar entre malware falso y el real; todos los usuarios deberían estar en conocimiento del problema de malware falso y qué hacer en caso de recibirlo;

l) aislar entornos donde pueden se pueden generar impactos catastróficos.

¿QUÉ ESTÁ HACIENDO MI UNIDAD TIC?

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

La Unidad TIC, implementará controles para prevenir y detectar código malicioso, lo cual se basa en software, concientización de usuarios y gestión del cambio. Los controles contemplan las siguientes directrices:

- Impedir el uso de software no autorizado.
- Impedir el compartir carpetas en los computadores y/o dispositivos personales.
- Implementar acciones y procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar en procedimientos de soporte a usuarios.
- Instalar y actualizar software de detección y reparación de virus, IPS de host, anti-spyware examinado computadores y medios informáticos, como medida preventiva y rutinaria.

¿QUÉ ESTÁ HACIENDO MI UNIDAD TIC?

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

La Unidad TIC, implementará controles para prevenir y detectar código malicioso, lo cual se basa en software, concientización de usuarios y gestión del cambio. Los controles contemplan las siguientes directrices:

- Mantener los sistemas con las últimas actualizaciones de seguridad disponibles, previa realización de pruebas en un ambiente dispuesto para tal fin.
- Chequear periódicamente el contenido de software y datos de los equipos de procesamiento, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
- Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
- Informar al personal acerca del problema de los falsos virus y de cómo proceder frente a los mismos.

¿QUÉ PUEDO HACER YO COMO USUARIO?

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

DEBO LEER Y RESPETAR LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

- ✓ Debo considerar todos los contenidos y las descargas como potencialmente inseguros hasta que no sean convenientemente analizados por una herramienta de detección de malware.
- ✓ Debo abstenerme de las siguientes acciones:
  - ➢ Ejecutar archivos descargados de servidores externos, de soportes móviles no controlados o adjuntos a correos, sin haber sido previamente analizados.
  - ➢ Configurar el programa cliente de correo electrónico para la ejecución automática de contenido recibido por correo.
  - ➢ Alterar la configuración de seguridad establecida para los sistemas y equipos de tratamiento de información.
  - ➢ Debo utilizarse únicamente el software permitido la institución. Este además debe estar convenientemente actualizado y licenciado [si no es así debe levantar una alerta interna].
  - ➢ Para evitar la recepción de spam se debo seguir las directrices incluidas en la política de correo electrónico.
  - ➢ No debo conectarme a mi equipo con permisos de “administrador”.

Ante cualquier duda, anomalía o sospecha de anormalidad en su equipo ES MI DEBER reportarlo de inmediato al Encargado de Ciberseguridad. No espere a que el problema empeore y afecte a toda la organización.

EL USUARIO ES NUESTRO ALIADO EN LA BATALLA CON LA CIBERDELINCUENCIA!!

¿QUÉ PUEDO HACER YO COMO USUARIO?

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

¡USTED ES NUESTRO ALIADO EN LA BATALLA CONTRA LOS CIBERINCIDENTE!

¿QUÉ PUEDO HACER YO COMO USUARIO?

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

¡LOS USUARIOS SOMOS EL PRIMER FRENTE DE DEFENSA CONTRA LOS CIBERATAQUES!

¿QUÉ PUEDO HACER YO COMO USUARIO?

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

¡NUESTRAS ACCIONES PUEDEN AYUDAR A PROTEGER LA INFORMACIÓN Y LOS SISTEMAS DE LA ORGANIZACIÓN!

¿QUÉ PUEDO HACER YO COMO USUARIO?

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

¡LA CIBERSEGURIDAD ES RESPONSABILIDAD DE TODOS!

¿QUÉ PUEDO HACER YO COMO USUARIO?

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

¡SEA USUARIOS RESPONSABLES Y AYUDEN A PROTEGER SU ORGANIZACIÓN Y SU HOGAR!

¿QUÉ PUEDO HACER YO COMO USUARIO?

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

¡JUNTOS, PODEMOS CREAR UNA ORGANIZACIÓN MÁS SEGURA!

Visítennos en

https://www.csirt.gob.cl

https://twitter.com/csirtgob

https://twitter.com/CSIRTConciencia

https://www.linkedin.com/in/csirt-gobierno-18584817b/

CSIRT
Gobierno de
Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.10.06 15:23:55 -03'00'