CAS-CHILE®
LÍDER EN SOFTWARE DE GESTIÓN PÚBLICA

RELACIONES ENTRE NORMAS Y EL SGSI

Ciberataques en la Actualidad

De acuerdo con la empresa de seguridad informática israelí, Check Point, en marzo de este año, los intentos de ciberataques en Chile casi se cuadruplicaron en solo dos semanas, posicionando al país como el cuarto entre los cinco con mayor aumento de intentos de ataques en el mundo.

Según las estadísticas, en la semana del 6 de marzo se registraron 1.116 ataques por organización en el país, mientras que en la semana iniciada el día 20 del mismo mes, la cifra aumentó a 4.245.

Como Protegernos de Ciberataques

- Mantenga el software y el sistema operativo actualizados
- Use software antivirus y manténgalo actualizado
- Use contraseñas seguras
- Nunca abra los archivos adjuntos de los correos electrónicos de spam
- No brinde información personal a menos que use un método seguro
- Comuníquese con el SGSI directamente para informar sospechas

Ciberseguridad en CAS-CHILE

LEY N°21.459

Ley de Delitos Informáticos

Norma que establece normas y sanciones sobre delitos informáticos.

ISO 27001

ISO/IEC 27001

Norma Internacional

Estandard que proporciona un marco de trabajo para los SGSI, con el fin de proteger Confidencialidad, Integridad y Disponibilidad.

SGSI

Sistema de Seguridad de la Información

Sistema que implementa y controla, la información en base a lo establecido en la norma.

ePULPO

ePULPO

Plataforma

Plataforma del Sistema de Gestión de Seguridad de la información que apoya al SGSI en el cumplimieinto de la norma.

LEY DE DELITOS INFORMATICOS

RECORDEMOS

La Ley N° 21.459 de delitos informáticos establece penas asociadas a actos ilícitos que afecten la información de la organización o de los clientes asociados a ella.

En la siguiente tabla se ejemplifica que punto de la tríada CID **(Confidencialidad, Integridad y Disponibilidad)** se ve afectado según la falta.

ARTICULOSDE LA LEY 21459	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
1. Ataque a la Integridad de un Sistema Informático	✖	✖	✖
2. Acceso Ilícito	✖	✖	
3. Interceptación Ilícita	✖	✖	✖
4. Ataque a la Integridad de los Datos Informáticos	✖	✖	
5. Falsificación Informática	✖	✖	
6. Receptación de Datos	✖	✖	✖
7. Fraude Informático	✖	✖	✖
8. Abuso de los Dispositivos	✖	✖	✖

PENAS ASOCIADAS

Tipos de Penas

Penas desde **61 días** a **10 años** de prisión

Multas desde **11** a **30 UTM**

Agravante:
Abuso de posición de confianza en la administración del sistema o custodio de datos informáticos

Buenas prácticas para no afectar la información

Uno de los objetivos de la **Norma ISO/IEC 27001** es resguardar la información de la organización y de los clientes asociados, bajo los tres pilares de la información (CID) **Confidencialidad, Integridad y Disponibilidad**. A continuación, se definen buenas prácticas para que no se vea afectada la información bajo estos tres conceptos.

CONFIDENCIALIDAD

- Emplear métodos de seguridad basados en roles para garantizar la autorización del usuario.
- Los controles de acceso aseguran que las acciones del usuario permanezcan dentro de sus roles.
- Un proceso de autenticación, que garantiza a los usuarios autorizados se les asignen identificaciones y contraseñas confidenciales.

INTEGRIDAD

- Cifrado de datos (bloquea datos por cifrado)
- Almacenar una copia de datos en una ubicación alternativa.
- Controles de acceso, incluida la asignación de privilegios de lectura o escritura.
- Validación de datos, para certificar transmisiones no corrompidas.

DISPONIBILIDAD

- Implementar medidas de seguridad para evitar interrupciones.
- Asegurar los datos en sistemas de almacenamiento
- Implementar procedimientos y políticas que pueden activarse en caso de fallas o incidentes de seguridad.

Dominios de Seguridad de la Información ISO/IEC 27001

La norma ISO 27001 establece 14 *dominios de seguridad de la información.*

A continuación, se presentan 5 de ellos, los que son considerados como esenciales para los colaboradores de CAS-CHILE.

5. Políticas de Seguridad

Deben cumplir con las Políticas establecidas por el SGSI

- AMSI-02 Medios Removibles
- AMSI-03 Seguridad de la Información en el Teletrabajo
- AMSI-04 Contraseña Segura
- AMSI-05 Dispositivos Móviles
- AMSI-06 Uso Aceptable de los Activos
- AMSI-07 Escritorio y Pantalla Limpia
- AMSI-08 Control de Accesos

8. Gestión Activos (AMSI-06-07-04-03)

Preocuparse de no incumplir con la política, es decir no instalar software prohibidos por CAS-CHILE además del cuidado de sus activos.

9. Control de Accesos (AMSI-08-04-03)

Al momento de su ingreso se establecieron credenciales de accesos lógicos para distintos servicios que le ayudaran a ejercer su labor en CAS-CHILE.

11. Seguridad Física y Ambiental (AMSI-08-06)

Al igual que los controles de accesos (lógicos), al incorporarse a CAS-CHILE se le hará entrega de una credencial de acceso físico es indispensable para su ingreso a las inmediaciones de la empresa.

12. Seguridad en la Operativa

Es importante que conozcan la importancia de completar un formato (fichas) con la información correcta, para dar fluides a los procesos.

PROCESO DISCIPLINARIO

El SGSI establece un proceso disciplinario enfocado en que los colaboradores cumplan con los controles mencionados anteriormente

SANCIONES: Al incumplir uno de los controles establecidos por la norma, se analizarán los hechos y gravedad de la falta, pudiéndose amonestar al o los trabajadores responsables.

Los grados de amonestación se establecen en base a lo estipulado en el **reglamento interno de CAS-CHILE®:**

Grado 1

Amonestación verbal.

Grado 2

Amonestación escrita con copia a la hoja de vida.

Grado 3

Amonestación escrita con copia a la hoja de vida del trabajador y al Inspector comunal del Trabajo.

Grado 4

Suspensión de funciones, sin remuneración, por hasta 3 días.

Grado 5

Multa de hasta un 25% de la remuneración diaria.

Grado 6

Término del Contrato de Trabajo.

Ventajas de un SGSI

Asegura Continuidad de Negocio

prepara a las organizaciones para reaccionar rápidamente ante cualquier amenaza, minimizando su impacto o incluso evitándolo.

Ventaja Competitiva

disponer de la certificación ISO/IEC 27001 puede convertirse en un elemento que diferencia una empresa de sus competidores fortaleciendo la confianza en la organización.

Genera procesos y procedimientos

óptimos, ofreciendo garantías de qué se debe realizar en cada situación, de qué forma y quien interactúa en cada caso.

Plataforma de Gestión - ePULPO

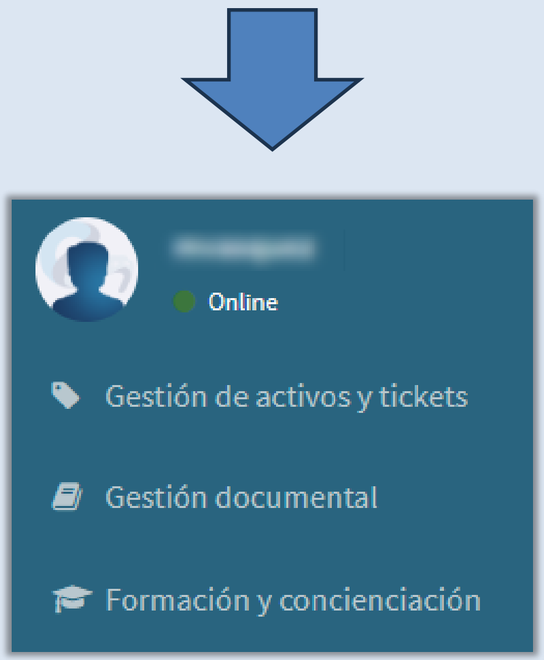
Para evitar sanciones y aprovechar las ventajas del SGSI la organización proporciona una plataforma de gestión llamada ePulpo, la cual está destinada a ayudar en la gestión del sistema en los siguientes puntos:

* Documentación
* Gestión de Tickets
* Control de Software e Inventario
* Formación y Concienciación
* Métricas
* Planes de Acción

Cumplimiento de la Ley

Las empresas evitan sanciones relacionadas con datos almacenados, privacidad y protección de datos, adecuando sus políticas de seguridad a las normativas y requisitos legales tanto nacionales como internacionales.

ePULPO



Gestión de activos y tickets

Dedicado a gestionar solicitudes, también denominados Tickets. En este apartado podrá crear peticiones asignándole una categoría como, por ejemplo:

* Solicitud de Entrega y devolución de equipo
* Instalación o aprobación de software
* Reparación de Equipo
* Sacar equipo de la empresa
* Solicitud de Acceso
* Solicitud de Alias

Gestión documental

En el apartado de Gestión Documental podemos encontrar toda la documentación que el SGSI dispone a sus colaboradores como, Instructivos, Formatos, Políticas y Procedimientos.

Formación y concienciación

Aquí podrá encontrar los modulo trimestrales realizados por el SGSI, Recordemos que bajo el punto auditable 7.2.2 Concienciación, educación y capacitación en seguridad de la información.

RECORDEMOS

Las personas somos el eslabón más importante de la ciberseguridad, ya que podemos cometer errores de manera inconsciente.

AGRADECEMOS SU ATENCIÓN

SGSI
CAS-CHILE

ÉXITO EN LA EVALUACIÓN