# Ciberdefensa Municipal

www.caschile.cl

Teléfono.
224966900

Email.
consultas@caschile.cl

Dirección
Marín 0586, Providencia, Chile.

# ¿Qué es Ciberdefensa municipal?

**Ciberdefensa municipal** es un conjunto de medidas y acciones destinadas a proteger la infraestructura tecnológica y la información de un municipio u organización de ataques cibernéticos.

# Escenario actual en Chile

Chile ostenta una de las mayores tasas de penetración de internet en América Latina, con más de un 90.02 % de su población conectada. Así lo certifica el informe Digital 2023 realizado por We Are Social y Hootsuite, Esta tasa elevada de usuarios con acceso a internet aumenta significativamente la vulnerabilidad.

En 2022 los ataques a instituciones públicas hicieron eco en las noticias debido lo expuesto que están los sistemas informáticos en Chile y la poca aplicación de medidas de seguridad.

# ¿Cómo proteger a tu organización?

Entre los servicios que puede ofrecer **Ciberdefensa municipal** se encuentran:

- Evaluación de riesgos
- Implementación de medidas de seguridad
- Monitoreo y análisis de incidentes
- Capacitación y concientización
- Respuesta a incidentes

**Ciberdefensa municipal** garantiza la protección de la infraestructura tecnológica y la información. Minimizando los riesgos y daños asociados a las ciberamenazas.

# Características principales

Nuestro producto contempla cuatro características principales, siendo capaz de analizar, detectar, defender y responder a las ciberamenazas. Protegiendo así los activos de información de tu municipio.

1 **Protección contra amenazas en línea**

2 **Protección perimetral**

3 **Monitoreo y gestión de Infraestructura TI**

4 **Detección y respuesta de amenazas**

# Beneficios

Podrás mantener los activos de tu municipalidad completamente protegidos de las amenazas actuales que afectan a las organizaciones públicas y privadas. De esta manera tendrás en tu organización una red segura y preparada ante incidentes de ciberseguridad. Entre los principales beneficios se encuentran:

- Protección contra cualquier tipo de malware.
- Monitoreo y análisis de incidentes de seguridad en tiempo real.
- Monitoreo en tiempo real de tu infraestructura TI.
- Análisis de vulnerabilidades en constante actualización.
- Detección de amenazas.
- Respuesta automatizada ante eventos de seguridad.
- Gestión centralizada.

## Servicios integrados en ciberdefensa municipal

| | |
|---|---|
| **Protección contra amenazas en línea** | • Protección antivirus y antimalware.<br>• Firewall individual.<br>• Control parental.<br>• Protección de la privacidad.<br>• Protección de la identidad.<br>• Optimización del sistema |
| **Protección perimetral** | • Protección firewall de alta velocidad.<br>• Prevención de intrusiones.<br>• VPN IPSec y VPN SSL.<br>• Filtro de contenido.<br>• Análisis de tráfico.<br>• Gestión de ancho de banda. |
| **Monitoreo y gestión de Infraestructura TI** | • Monitoreo de la infraestructura en tiempo real.<br>• Monitoreo de Windows.<br>• Monitoreo de servidores y servicios.<br>• Monitoreo de aplicaciones. |
| **Detección y respuesta de amenazas** | • Monitoreo de seguridad en tiempo real.<br>• Detección de amenazas.<br>• Respuesta automática a incidentes.<br>• Análisis de vulnerabilidades.<br>• Gestión de políticas de seguridad. |

# Servicios adicionales

CAS-CHILE considera fundamental brindar capacitación y conciencia en ciberseguridad a los empleados de las organizaciones para que puedan proteger la infraestructura y la información de una forma correcta. La adaptación de los servicios a las necesidades y presupuestos de cada municipio es importante para que las organizaciones comprendan los beneficios que pueden obtener.

| | |
|---|---|
| **Gestión de Ciberactivos** | Establecer una cibergestión sólida a través de la identificación, evaluación e implementación de medidas de seguridad. Se monitorean y analizan las amenazas para asegurar una respuesta eficaz contra ellas, y se educa y concientiza a los perfiles sobre las buenas prácticas de seguridad y la sensibilización sobre los riesgos para prevenir incidentes. |
| **Gestión de riesgos** | Identificar, evaluar y mitigar los riesgos que podrían afectar sus ciberactivos de información y su capacidad para cumplir los objetivos. Al implementar un enfoque sistemático para la gestión de riesgos, las organizaciones pueden tomar decisiones informadas y reducir la exposición a posibles amenazas y riesgos. |
| **Políticas de seguridad de la información** | Creación de normas, procedimientos y directrices claras y completas son esenciales para proteger los activos digitales de una organización y reducir los riesgos de seguridad. Las políticas de seguridad de la información deben establecer el propósito y alcance, definir responsabilidades y obligaciones, cumplir con leyes y regulaciones aplicables, monitorear y hacer cumplir las políticas, así como actualizarlas y mantenerlas adecuadamente. |
| **Análisis de Impacto del Negocio (BIA)** | Identificar los procesos y sistemas críticos de la organización, y evaluar el impacto financiero, legal, operativo y reputacional de una interrupción o desastre. Ayudando a priorizar recursos y a planificar la continuidad del negocio y un plan de recuperación ante desastres para así mejorar la gestión de riesgos. |
| **Procedimientos de Gestión de Incidentes** | Establecer una guía clara y estructurada para detectar, reportar, analizar y resolver incidentes de seguridad en un sistema o red de manera rápida y efectiva. El objetivo es minimizar el impacto y los daños causados por los incidentes, restaurar los servicios afectados lo antes posible y prevenir futuros incidentes similares. |