prey

## Guía de cumplimiento con la

# ley 21.663

## para el sector TI

Prey Inc.

# Industria TI: Sistema nervioso de la economía

Todo negocio moderno late al ritmo de sus equipos y plataformas informáticas. Basta que un servidor crítico se caiga o que un sistema de autenticación falle para que el corazón corporativo entre en paro. Las áreas de TI no solo mantienen las luces encendidas: custodian credenciales de usuarios, bases de datos repletas de información sensible, código fuente con años de desarrollo y secretos de infraestructura que, en las manos equivocadas, se vuelven un tesoro para los cibercriminales. Esa combinación de acceso y control convierte a la industria de TI en uno de los objetivos más jugosos para atacantes que buscan abrirse paso en organizaciones enteras.

Los ataques recientes a MSPs globales como SolarWinds, Kaseya y MOVEit, sumados a incidentes locales en Chile como al grupo GTD, dejaron claro que basta comprometer a un solo proveedor para que la reacción en cadena afecte a cientos de clientes de distintas industrias. Es por eso que la Ley 21.663 no se anda con rodeos: considera a los operadores y proveedores de servicios digitales críticos como piezas esenciales de la seguridad nacional.

**Aumento de hackeos en Chile: alerta por ciberataques y suplantación**

**Aumento de los ciberataques en Chile en 2023: Lo que dicen las cifras, las formas más frecuentes y las consecuencias**

**Chile es el segundo país de la región con más ciberataques este año: suma más de un millón**

**El auge de los ciberataques en Chile: fuga de datos afecta al 60% de las empresas y experta llama a “estar alertas”**

**Sabías que?**

Según Fortinet, Chile sufrió en el 2024 más de 27,600 millones intentos de ciberataques, posicionándose como el segundo país de la región con más ciberataques.

# 01

## ¿Mi organización está obligada a cumplir?

# ¿Mi organización está obligada a cumplir?

Si tu negocio forma parte del ecosistema tecnológico —proveedor cloud, MSP, MSSP, integrador, desarrollador SaaS o data center— es posible que ya seas un Operador de Servicios Esenciales (OSE) o incluso un Operador de Importancia Vital (OIV). Pero no termina ahí: la ANCI también puede designar como OIV a instituciones privadas que, aunque no sean OSE, cumplen un rol estratégico en el país y cuyo fallo podría afectar a miles de usuarios.

Para definir si un servicio es esencial o de importancia vital, la ANCI sigue un proceso que considera el impacto potencial de una interrupción y la dependencia de redes y sistemas TI críticos.

## Este procedimiento incluye:

1. Solicitar informes a organismos públicos con competencia en el sector.
2. Elaborar una nómina preliminar de instituciones candidatas.
3. Someter la lista privada a consulta pública por 30 días.
4. Recibir informe del Ministerio de Hacienda sobre las entidades públicas.
5. Emitir una resolución final que establece oficialmente a los OIV.

## Quienes están dentro del sector TI según la ley?:

- **Empresas que ofrezcan servicios digitales (IaaS, PaaS, SaaS):** Proveedores que ofrecen infraestructura, plataformas y software como servicio, fundamentales para operaciones empresariales y gubernamentales.
- **Empresas que ofrezcan servicios de infraestructura digital:** Proveedores que sostienen la conectividad y el procesamiento de datos en el país tales como data centers, alojamiento de servidores o servicios de red y conectividad crítica (IXPs, backbone IP).
- **Empresas que ofrezcan servicios de tecnología de la información gestionada por terceros (MSP / MSSP):** Proveedores que ofrecen gestión de infraestructura de TI y seguridad de forma remota a terceros.

## Otras subindustrias que podrían entrar bajo ciertas condiciones:

**Empresas que desarrollan o mantienen software esencial para sectores críticos**

- Software para hospitales, bancos, servicios de emergencia, etc.
- Si su interrupción implica un impacto societal significativo.

**Plataformas tecnológicas que actúan como infraestructura base para servicios esenciales**

- EdTech para educación pública masiva.
- HealthTech usada por la red pública de salud.
- FinTech que provee servicios a bancos estatales o pagos del Estado.

**Integradores o consultoras que operan infraestructura de terceros esencial**

- Si tienen control operativo sobre sistemas críticos, aunque no sean los dueños (especialmente aplicable si prestan servicios a OSE, OIV o instituciones públicas)

## Qué pasa si aún no estás designado oficialmente

Aunque tu organización no haya sido designada oficialmente como OSE u OIV, eso no significa que en un futuro no pueda ser catalogada como tal. La ANCI revisa y actualiza las designaciones cada tres años, y una afectación significativa —como un ciberataque a tu infraestructura o la caída de servicios críticos que afecten a clientes OSE/OIV— podría hacer que pases a estar en la lista.

Prepararse desde ya es una ventaja para evitar sorpresas y responder mejor ante incidentes. En el sector TI, esto es aún más relevante porque muchas empresas gestionan y protegen sistemas y assets críticos que pueden convertirse en puntos únicos de falla para múltiples industrias.

## Auto-chequeo express (responde SÍ/NO)

| Pregunta | "sí" significa... |
|---|---|
| **¿Provees servicios cloud, hosting, SaaS, data center o conectividad a terceros?** | Eres OSE; regístrate ya en portal.anci.gob.cl |
| **¿Gestionas infraestructuras o endpoints críticos para clientes (MSP, MSSP, integrador)?** | Puedes ser nombrado OIV por arrastre; mismas multas |
| **¿Eres el departamento TI de una compañía clasificada como OSE u OIV (banca, salud, educación, energía, gobierno)?** | Mismo régimen de obligaciones y fiscalización |
| **¿Una caída total dejaría sin servicio a más de una región o pondría vidas en riesgo?** | Criterio de impacto nacional → probable OIV |
| **¿Dependemos de un único SCADA, datacenter tier III+ o sistema OT cuya falla frene todo?** | Punto único de falla: foco directo de fiscalización |
| **¿Hemos recibido un oficio o encuesta de la ANCI/CSIRT pidiendo información?** | Estás en proceso formal de calificación: prepara SGSI y delegado hoy |

### A tomar en cuenta

- **3 o más "SÍ":** Actúa desde ahora como OSE/OIV; las sanciones (hasta 40 000 UTM) aplican desde marzo 2025.
- **1-2 "SÍ":** Implementa controles básicos y mantente alerta a nuevas resoluciones de la ANCI.
- **0 "SÍ":** Mantén buenas prácticas; la lista se actualiza cada tres años.

## Consideraciones especiales para PYMEs y proveedores TI críticos

Si eres una PYME tecnológica o proveedor en la cadena de suministro de servicios digitales esenciales, podrías verte afectado indirectamente. Aunque la ley contempla tu tamaño y capacidades, es clave demostrar buenas prácticas de ciberseguridad para no convertirte en el eslabón débil que exponga a los grandes operadores. Esto también puede abrirte puertas en contratos y licitaciones.

### Recomendaciones prácticas:

- Identificar si tus clientes principales son OSE u OIV.
- Designar un responsable TI con autoridad suficiente.
- Adoptar soluciones asequibles como MDM, antivirus, gestión de contraseñas, firewalls y backups automáticos.
- Capacitar al equipo en ciberhigiene básica (phishing, contraseñas seguras, etc.).
- Documentar procesos de seguridad, aunque sean simples.
- Tener un plan de continuidad operativa y respuesta a incidentes.
- Explorar certificaciones o estándares simplificados como ISO 27001 para PYMEs.


# 02

## Riesgos frecuentes en operaciones TI

# Riesgos frecuentes en operaciones TI

Las áreas de TI se enfrentan cada día a amenazas que van mucho más allá de un antivirus desactualizado. Los ataques modernos apuntan a los puntos ciegos: proveedores externos, credenciales olvidadas, configuraciones mal hechas y endpoints que nadie recuerda haber registrado. Según el Data Breach Investigation Report 2025, más del 60% de las brechas en servicios IT involucraron la explotación de terceros o errores humanos, un recordatorio brutal de lo fácil que es ser la puerta de entrada.

### Ataques a la cadena de suministro

Los cibercriminales infiltran librerías open-source o scripts posventa para distribuir código malicioso sin levantar sospechas. El DBIR 2025 destaca que el 15% de las brechas globales involucraron compromisos en la cadena de suministro, afectando especialmente a sectores con alta dependencia de terceros.

### Secuestro de credenciales privilegiadas

Ya sea por phishing o compra de datos en foros de la dark Web, las credenciales de administradores siguen siendo el premio mayor. El DBIR muestra que las credenciales robadas están presentes en el 31% de los incidentes analizados, con un impacto desproporcionado en negocios TI.

### Ransomware en servidores y backups

No solo cifran datos: ahora exfiltran información sensible para chantajear por partida doble. El informe revela que el ransomware representa casi el 44% de las brechas en empresas tecnológicas, afectando a servidores de producción y sistemas de respaldo por igual.

### Shadow IT y endpoints remotos

Dispositivos fuera del inventario oficial, como laptops en home office o servicios cloud no autorizados, son una mina para los atacantes.

### Errores de configuración en IaC

Un bucket S3 público, una base expuesta o una VM sin firewall pueden abrir la puerta a un desastre. El DBIR señala que los errores de configuración son responsables del 29% de las brechas relacionadas con entornos cloud, un problema creciente con la adopción de IaC.

# 03 Obligaciones principales según la ley

# Obligaciones principales según la ley

La Ley 21.663 (artículo 8) establece un conjunto de obligaciones diseñadas para que las organizaciones críticas puedan prevenir, detectar y responder a incidentes de ciberseguridad. También obliga a reportar al CSIRT nacional cualquier incidente con efectos significativos en sus operaciones, algo que en el sector TI puede ser tan simple como un ransomware que deje inoperativos los sistemas de soporte a clientes o un error de configuración que exponga datos en la nube.

Aunque las medidas se dirigen principalmente a los Operadores de Servicios Esenciales (OSE) y Operadores de Importancia Vital (OIV), empresas TI que gestionan infraestructuras críticas, proveen servicios cloud, SaaS o datacenter, o que forman parte de la cadena de suministro de un OSE/OIV, podrían ser incluidas por la ANCI si un ataque compromete su funcionamiento o el de sus clientes.

## A continuación, las principales obligaciones:

### Registro obligatorio en el portal ANCI

OSE : ✓ | OIV: ✓

Todos los OSE y OIV deben registrarse en la plataforma oficial de la ANCI. Para empresas TI, este registro es el primer paso para que la Agencia pueda coordinar acciones, supervisar su ciberseguridad y notificarles sobre protocolos aplicables. Un registro actualizado demuestra proactividad y puede ser clave para evitar sanciones por omisión.

Desde el 11 de junio de 2025 ya se encuentra abierto el portal ANCI:
**portal ANCI:**

### Designación de delegado de ciberseguridad

OSE : ✓ | OIV: ✓

El delegado será el punto de contacto con la ANCI. En el sector TI, este rol suele recaer en un CISO, un vCISO externo o incluso en un jefe de operaciones con experiencia en seguridad. Su misión: coordinar respuestas, liderar auditorías y gestionar incidentes como brechas de datos de clientes o interrupciones en servicios SaaS críticos.

### Implementación de un SGSI activo y documentado

OSE : ✗ | OIV: ✓

Para los OIV, la ley exige un Sistema de Gestión de Seguridad de la Información (SGSI) que sea más que un stack de políticas olvidadas en un drive. En empresas TI esto significa gestionar riesgos en plataformas multitenant, redes híbridas, entornos de desarrollo y endpoints distribuidos, asegurando continuidad operativa aun cuando algo explote.

**Aprende cómo aplicar un SGSI en entornos TI:**
**Guía práctica sobre SGSI e ISO 27001**

### Reporte de incidentes (plazo: 3 horas)

OSE : ✓ | OIV: ✓

Si ocurre un ataque significativo —por ejemplo, ransomware que bloquea un panel de control de clientes o phishing masivo a cuentas de administradores— debes notificarlo al **CSIRT Nacional** en el portal de ANCI:

- 3 horas para la alerta temprana.
- 72 horas para actualizar la evaluación inicial, gravedad e IoC.
- 15 días para entregar el informe final.

El reporte sigue un formato XML con taxonomía ANCI.
**Decreto N° 295 | Resolución N° 7/2025**

### Auditorías, análisis de riesgos y simulacros

OSE : ✗ OIV: ✓

Las auditorías y simulacros no son solo ejercicios para cumplir. Para proveedores TI, esto puede incluir simulaciones de ataques de ransomware en infraestructura crítica, pruebas de restauración de backups o análisis de fallos en pipelines CI/CD.

### Planes de continuidad operacional y ciberseguridad

OSE : ✗ OIV: ✓

Un plan de continuidad bien diseñado permite a las empresas TI mantener activos servicios cloud o APIs críticas incluso durante una crisis. La ley exige revisarlos al menos cada dos años.

**Recomendamos:**
**Crea tu plan de respuesta a incidentes de ciberseguridad**

### Medidas para reducir impacto y propagación

OSE : ✗ OIV: ✓

En incidentes activos, se debe actuar rápido: aislar máquinas virtuales comprometidas, bloquear cuentas afectadas o desconectar redes de staging y producción para contener el daño.

### Certificaciones según el artículo 28

OSE : ✗ OIV: ✓

Se exige certificación como ISO 27001 para demostrar que el SGSI y los planes funcionan en la práctica. Para proveedores TI que no son OIV, adoptar controles ISO/NIST igual les aporta ventajas competitivas al mostrar compromiso con la seguridad.

### Notificación a potenciales afectados

OSE : ✗ OIV: ✓

Si un ataque expone datos sensibles (credenciales API, contratos, información de clientes), la empresa debe notificar a los afectados cuando pueda identificarlos.

### Programas de capacitación y campañas de ciberhigiene

OSE : ✗ OIV: ✓

Capacitar a los equipos DevOps, soporte y administración es vital para reducir el error humano, la causa raíz del 68% de las brechas según el DBIR 2025. Desde phishing hasta manejo de accesos privilegiados, estas campañas pueden marcar la diferencia.

### Cumplimiento de normativas técnicas ANCI o sectoriales

OSE : ✓ OIV: ✓

Adoptar estándares técnicos (ISO 27001, NIST CSF, CIS Controls) asegura que sistemas y procesos estén alineados con las mejores prácticas y listos para inspecciones.

**Recursos adicionales:**
**Checklist descargable: Simplifica el cumplimiento paso a paso para empresas TI.**

# 04

## Qué pasa si no cumples

# Qué pasa si no cumples

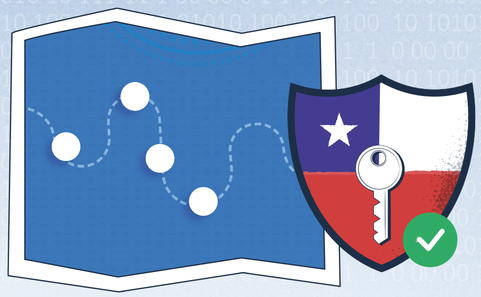
La Ley Marco de Ciberseguridad no se anda con rodeos cuando se trata de sanciones. Clasifica las infracciones en tres niveles: leves, graves y gravísimas, según la gravedad del incumplimiento y el impacto potencial. En el mundo TI, esto puede ir desde retrasos en enviar datos a la ANCI hasta la omisión de reportes sobre un ransomware que dejó inoperativo un servicio SaaS para cientos de clientes.

| Tipo de infracción | Definición breve | Multa máxima (OSE) | Multa máxima (OIV) |
|---|---|---|---|
| **Leve** | Retrasos en reportes no críticos o incumplimientos menores. | 5.000 UTM | 10.000 UTM |
| **Grave** | No implementar estándares, omitir reportes críticos, entorpecer fiscalizaciones. | 10.000 UTM | 20.000 UTM |
| **Gravísima** | Reincidir en infracciones graves o no contener un incidente de alto impacto. | 20.000 UTM | 40.000 UTM |

## Tipos de infracciones según el artículo 38

| Categoría Infracciones | Infracciones OSE | Infracciones OIV |
|---|---|---|
| **Infracciones Leves** | • Entregar fuera de plazo la información solicitada, siempre que no sea crítica para la gestión de un incidente.<br>• Incumplir instrucciones de la ANCI cuando no constituyan una infracción grave o gravísima.<br>• Cualquier otra infracción sin sanción especial definida en la ley. | • No mantener el registro de las acciones de seguridad realizadas.<br>• No comunicar al CSIRT Nacional sobre revisiones y ejercicios continuos.<br>• No implementar programas de capacitación y educación continua en ciberseguridad.<br>• No designar un delegado de ciberseguridad.<br>• Incumplir con la certificación de planes de continuidad operacional.<br>• No contar con las certificaciones exigidas por la ley. |
| **Infracciones Graves** | • No implementar los protocolos y estándares de la ANCI para gestionar ciberincidentes.<br>• No aplicar los estándares sectoriales de ciberseguridad.<br>• Entregar fuera de plazo información necesaria para gestionar un incidente.<br>• Presentar información falsa o errónea a la ANCI.<br>• Omitir el reporte obligatorio de incidentes (artículo 9°).<br>• Negarse sin justificación a cumplir instrucciones o entorpecer la labor de la ANCI durante un incidente.<br>• Reincidir en una infracción leve dentro de un año. | • No implementar un SGSI continuo.<br>• No elaborar ni ejecutar los planes de continuidad operacional y ciberseguridad.<br>• No informar a los afectados sobre incidentes que comprometan datos críticos.<br>• No tomar medidas rápidas para contener y reducir el impacto de un incidente o ciberataque.<br>• Reincidir en una infracción leve dentro de un año. |
| **Infracciones Gravísimas** | • Entregar información falsa o errónea a la ANCI cuando sea crucial para la gestión de un incidente significativo.<br>• Desobedecer instrucciones de la ANCI durante un incidente de alto impacto.<br>• Negarse a entregar información esencial para incidentes significativos.<br>• Reincidir en una infracción grave dentro de un año. | • No aplicar medidas de contención en incidentes de impacto significativo.<br>• Reincidir en una infracción grave dentro de un año. |

# 05



## Pasos prácticos para cumplir con la Ley 21.663

# Pasos prácticos para cumplir con la Ley 21.663

Aquí tienes un punto de partida claro: una hoja de ruta con los pasos clave para levantar un SGSI, elegir las herramientas correctas y preparar a tu equipo para los retos de la Ley 21.663. Piensa en esto como el checklist que todo proveedor TI, MSP o equipo de infraestructura debería tener a la vista para no quedarse atrás. ¿Listo para ponerte manos a la obra?

## Plan de implementación por fases

Intentar desplegar un SGSI completo de una sola vez puede ser como hacer un rollback en producción... sin backup. Es abrumador, costoso y casi siempre acaba en retrasos. La mejor estrategia es dividir el proyecto en fases manejables, priorizando lo más crítico. Así puedes gestionar recursos de forma eficiente, mostrar avances rápidos a dirección y ajustar sobre la marcha antes de una implementación total.

| Fases | Nombre | Descripción |
|---|---|---|
| **Fase 1** | Diagnóstico y planificación | Realiza un mapeo de activos (on-prem y cloud), define el alcance del SGSI y asigna responsables. |
| **Fase 2** | Políticas y procedimientos básicos | Redacta políticas para control de accesos, gestión de vulnerabilidades y respuesta a incidentes. |
| **Fase 3** | Controles técnicos iniciales | Implementa MFA, backups 3-2-1, segmentación de redes y un inventario actualizado de endpoints. |
| **Fase 4** | Formación y concientización | Capacita a equipos DevOps y de soporte en prácticas seguras (secrets management, phishing). |
| **Fase 5** | Auditorías internas y ajustes | Ejecuta auditorías tipo “tabletop”, revisa logs SIEM y corrige brechas antes de la certificación. |

## Diagnóstico inicial

Antes de lanzarte a comprar un firewall next-gen o contratar un vCISO, necesitas saber dónde estás parado. El diagnóstico inicial es como un escaneo completo de tu organización: revela activos críticos, mapea riesgos y muestra las brechas que podrían costarte caro en una auditoría de la ANCI.

**Recursos adicionales:**

- Cómo implementar un programa de gestión de riesgos
- Matriz de riesgos: Guía para lideres de TI

## Pasos del diagnóstico inicial:

1. **Inventario de activos:** Haz un inventario completo de todo lo que forma el ADN de tu operación TI: servidores on-prem y en la nube, endpoints remotos (sí, esas laptops olvidadas en home office cuentan), redes, aplicaciones SaaS, APIs, contenedores y datos sensibles. Este mapa es fundamental para saber qué proteger y descubrir qué tan expuesto está tu stack actual.
2. **Análisis de riesgos:** No basta con listar activos; hay que entender qué podría salir mal. Realiza un análisis de amenazas internas (errores de configuración, Shadow IT) y externas (ransomware, ataques a la cadena de suministro). Evalúa la probabilidad e impacto de cada riesgo, desde la caída de un cluster Kubernetes hasta el secuestro de credenciales de administración. Esta información será tu brújula para priorizar controles y cerrar los huecos más peligrosos primero.
3. **Revisión de políticas actuales:** Haz un inventario de las políticas y procedimientos de seguridad que ya existen en tu organización. ¿Tienes un manual de contraseñas, un plan de respuesta a incidentes o reglas para el manejo de datos en la nube? Ahora pregúntate: ¿cubren realmente los riesgos modernos como DevOps mal asegurados, APIs expuestas o Shadow IT? ¿Están alineadas con estándares como ISO 27001 o NIST CSF? Este análisis permite detectar vacíos críticos y ajustar la gobernanza antes de lanzarte a implementar un SGSI.
4. **Mapeo de procesos:** Mira cómo fluye la información dentro de tu operación TI: quién tiene acceso a credenciales privilegiadas, cómo se comparten los datos entre entornos dev, test y prod, y dónde pueden existir cuellos de botella o puntos únicos de falla (como un admin root sin MFA). El objetivo es visualizar los flujos de trabajo y ubicar procesos que necesitan controles adicionales para blindar la integridad y confidencialidad de los datos.
5. **Reporte de brechas:** Elabora un informe claro con las brechas y vulnerabilidades detectadas en los pasos anteriores. Prioriza áreas críticas como gestión de accesos, backups y segmentación de redes, según el riesgo e impacto potencial. Este documento no solo será la base de tu plan de acción; también te ayudará a convencer a dirección y al CFO de que invertir en seguridad ahora evita multas y pérdidas de clientes más adelante.

## Designación del delegado

Una vez que sabes dónde estás, toca nombrar a la persona que liderará el cambio. La ley exige como mínimo un delegado de ciberseguridad como punto de contacto con la ANCI, pero en organizaciones TI grandes (MSPs, datacenters, SaaS) es recomendable tener un encargado de ciberseguridad y armar un equipo de apoyo.

Este equipo puede incluir al CISO, responsables de infraestructura y líderes DevOps para que el delegado no cargue solo con toda la gestión, monitoreo y notificación de incidentes. Este rol será clave para coordinar acciones, alinear el SGSI con las operaciones diarias y asegurarse de que las políticas no queden como un PDF olvidado en un repositorio.

## Evaluación y selección de un marco SGSI (ISO/NIST)

Elegir un marco sólido es como definir el blueprint de tu ciberseguridad. Si eres proveedor de servicios cloud, MSP o gestionas infraestructuras críticas, esta decisión marcará la diferencia al estructurar tu SGSI y cumplir con la Ley 21.663. Aunque hay varias opciones, **ISO 27001** destaca porque es el estándar que la normativa chilena toma como referencia.

Además, facilita auditorías, contratos con clientes internacionales y la obtención de certificaciones que generan confianza. Por otro lado, **NIST CSF** puede complementar muy bien si operas en EE. UU. o trabajas en entornos con alta carga técnica, como DevOps y OT.

| Aspecto | ISO 27001 | NIST Cybersecurity Framework |
|---|---|---|
| **Enfoque** | Sistema de gestión completo basado en ciclo PDCA (Plan-Do-Check-Act). | Buenas prácticas y controles flexibles para gestión de riesgos. |
| **Certificación** | Certificable a nivel internacional; ideal para contratos con grandes clientes. | No certificable, funciona como guía voluntaria. |
| **Alineación con Ley 21.663** | Totalmente alineado; la ley lo menciona como referencia principal. | Complementa ISO pero no lo reemplaza. |
| **Cobertura geográfica** | Reconocido globalmente, útil para SaaS y MSPs con operaciones internacionales. | Predominante en EE. UU. y sectores técnicos como infraestructuras OT. |
| **Uso ideal** | Empresas que buscan un SGSI estructurado, auditado y listo para certificación. | Equipos que requieren agilidad y guías prácticas para fortalecer controles. |

## Automatización de alertas y trazabilidad

En operaciones TI, el tiempo de reacción lo es todo. Una brecha no detectada puede pasar de molesta a desastrosa en cuestión de minutos. Por eso, automatizar alertas es clave para cazar anomalías antes de que escalen. Y no olvides la trazabilidad: la Ley 21.663 exige registros detallados para demostrar que tomaste acción cuando tocaba.

| Elemento | ¿Qué es? | ¿Qué ofrece? | ¿Qué aporta? | Cómo y con qué app |
|---|---|---|---|---|
| **Automatización de alerta** | Sistemas que notifican automáticamente al detectar comportamientos sospechosos o cambios críticos (ej. acceso no autorizado a un cluster Kubernetes). | Alertas en tiempo real vía email, SMS o dashboards, para que tu equipo reaccione antes de que el daño sea irreparable. | Reduce drásticamente los tiempos de respuesta y frena ataques antes de que comprometan datos o sistemas. | SIEM como Splunk o Sentinel para eventos complejos. Con Prey, configura reglas automáticas (geofencing, batería baja, cambios de hardware) para recibir notificaciones instantáneas y ejecutar acciones remotas (bloqueo/ borrado). |
| **Trazabilidad** | Registro continuo y detallado de eventos y acciones de seguridad: quién hizo qué, cuándo y cómo. | Logs completos con fechas, responsables y resultados para cumplir con la Ley 21.663 y auditorías. | Permite reconstruir la cadena de eventos tras un incidente y probar cumplimiento frente a la ANCI o clientes. | Plataformas como Vanta o Drata centralizan logs y generan reportes automáticos. Prey guarda historial de bloqueos, recuperaciones y cambios para evidencias claras. |

## Capacitación y concientización interna

Puedes tener el mejor firewall del mercado y una flota de endpoints protegida con EDR, pero si alguien en tu equipo hace clic en un enlace de phishing, las puertas al desastre quedan abiertas.

La formación continua no es opcional: es tu mejor defensa contra errores humanos, que el **DBIR 2025** identifica como la causa en **el 60% de las brechas**. En empresas TI, donde los permisos de administración y los accesos a infraestructuras críticas abundan, un equipo bien entrenado es un escudo activo contra ataques.

### Ideas y plataformas para capacitar a tu equipo

- **Simulaciones de phishing**
  Lanza campañas falsas de phishing para entrenar al staff técnico y no técnico en detectar correos maliciosos antes de que comprometan credenciales privilegiadas.

  **Plataforma recomendada:** KnowBe4, Proofpoint Security Awareness.

- **Cursos interactivos de ciberseguridad**
  Ofrece módulos cortos sobre higiene digital, gestión segura de contraseñas, y buenas prácticas en DevOps (manejo de secrets, revisión de código).

  **Plataforma recomendada:** Udemy for Business, Coursera, o incluso módulos internos vía GitHub Learning Lab.

- **Cartelería digital y recordatorios**
  Refuerza mensajes clave en herramientas de colaboración como Slack, Microsoft Teams o a través de dashboards internos (p. ej., “¿Rotaste tus claves SSH este mes?”).

  **Plataforma recomendada:** Slack workflows, Microsoft Viva.

- **Simulacros de incidentes**
  Realiza ejercicios prácticos tipo “tabletop” donde el equipo responde a un ransomware que compromete servidores SaaS o un fallo en la cadena CI/CD.

  **Plataforma recomendada:** Cyberbit, RangeForce.

## Define tu plan de continuidad operativa (PCO) y respuesta ante incidentes

Cuando algo falla —y en TI tarde o temprano falla— lo importante no es solo evitarlo, sino saber cómo reaccionar. La Ley 21.663 exige un PCO para asegurar que los servicios esenciales sigan funcionando tras un ciberataque. Aquí es donde entra ISO 22301, el estándar clave en continuidad de negocio.

### ¿Qué involucra un PCO y un plan de respuesta ante incidentes

- **Identificación de procesos críticos:** Define qué sistemas no pueden parar (p. ej., APIs para clientes, servidores de autenticación, infraestructuras cloud multitenant).
- **Evaluación de riesgos y análisis de impacto:** Escenarios como caída de datacenters, fuga de datos de clientes o corrupción de backups.
- **Protocolos de respuesta rápida:** Contención de servidores comprometidos, aislamiento de redes, y reportes al CSIRT Nacional en menos de 3 horas.
- **Roles y responsabilidades:** Desde el líder de ciberseguridad hasta el equipo de soporte, todos deben saber qué hacer y cuándo.
- **Pruebas y simulacros periódicos:** Validar que los planes funcionan bajo presión y con tiempos cronometrados.
- **Planes de recuperación:** Estrategias para restaurar servicios SaaS, bases de datos o entornos de desarrollo a pleno rendimiento.
- **Lecciones aprendidas:** Tras cada incidente o simulacro, revisa qué funcionó y qué no para reforzar la postura de seguridad.

## Pruebas, simulacros y auditorías

Tener un plan en papel está bien, pero ¿funciona en producción? Las pruebas, simulacros y auditorías son el único modo de saberlo. En entornos TI, esto puede implicar desde restaurar backups en tiempo real hasta ejecutar ataques simulados en entornos sandbox para evaluar tiempos de respuesta. Además, la Ley 21.663 exige revisiones mínimas cada dos años para mantener la operatividad y la certificación.

| Elemento | ¿Qué es? | ¿Qué aporta? | ¿Qué involucra? |
|---|---|---|---|
| **Pruebas** | Ejecuciones controladas de sistemas y procesos para validar su resiliencia. | Detecta fallos técnicos o configuraciones incorrectas antes de un incidente real. | Revisar backups, probar failovers en clusters, validar triggers de alertas en SIEM y EDR. |
| **Simulacros** | Ejercicios prácticos donde los equipos simulan responder a ataques. | Entrena al personal y mide la coordinación bajo presión. | Escenarios como ransomware en pipelines CI/CD o ataques DDoS; tiempos de contención cronometrados. |
| **Auditorías** | Evaluaciones formales y periódicas del cumplimiento de políticas y normativas. | Proporciona evidencia para ANCI y asegura alineación con ISO 27001/22301 y la Ley 21.663. | Auditorías internas y externas, revisión de logs, entrevistas a responsables, análisis de incidentes pasados. |

## Documentación y evidencia

En ciberseguridad, lo que no está documentado simplemente “no existe” para un auditor... ni para la ANCI. La Ley 21.663 exige mantener registros claros y actualizados que demuestren la aplicación real de medidas de seguridad. Esto también es vital para reconstruir incidentes (¿quién accedió al clúster de producción? ¿qué cambios hubo en la infraestructura?) y para mantener la confianza de tus clientes.

### Documentación clave que deberías tener lista en tu operación TI:

- **Políticas y procedimientos**
  - Política de seguridad de la información (actualizada cada año).
  - Procedimientos de gestión de incidentes (desde ransomware en servidores hasta fuga de API keys).
  - Planes de continuidad operativa y recuperación de desastres (especialmente para servicios SaaS).
- **Registros de actividades**
  - Logs de acceso a sistemas críticos y cuentas privilegiadas.
  - Historial de configuraciones en infraestructuras como código (IaC).
  - Ejecuciones de acciones remotas con herramientas como **Prey** (bloqueos, borrados, geofencing).
- **Evidencia de capacitación**
  - Listados de sesiones y contenidos impartidos.
  - Certificados de participación de equipos técnicos y administrativos.
  - Resultados de campañas de phishing y métricas de mejora (ej. menos clics en enlaces fraudulentos).
- **Informes de auditorías y simulacros**
  - Auditorías internas y externas completas, con hallazgos y planes de acción.
  - Resultados de simulacros de ciberataques en infraestructuras cloud o entornos DevOps.
  - Lecciones aprendidas y ajustes implementados.
- **Certificaciones y cumplimiento**
  - Certificados ISO 27001 o ISO 22301 (si ya los tienes).
  - Evidencia de revisiones periódicas y reportes enviados a la ANCI o CSIRT Nacional.
- **Inventario de dispositivos y quienes lo manejan**
  - Laptops y desktops corporativos, incluyendo endpoints BYOD bajo control MDM.
  - Dispositivos móviles (smartphones, tablets) y quién los usa.
  - Servidores (físicos y cloud), redes (routers, firewalls), IoT críticos (cámaras, sensores).
  - Medios de almacenamiento externo (USBs, discos duros, cintas de backup).

## Implementación de políticas y controles

Aquí es donde se pasa del plan al código real... o al control real. Un SGSI efectivo necesita políticas claras sobre quién tiene acceso a qué y controles técnicos que las respalden.

### Ejemplos clave para un entorno TI:

- **Gestión de accesos basados en roles (RBAC):** Define permisos mínimos según el rol: los desarrolladores no deberían tener acceso directo a bases de datos en producción, y los operadores no necesitan claves root en servidores.
- **Política de contraseñas y MFA:** Fuerza contraseñas robustas y autenticación multifactor en todos los accesos críticos (VPN, paneles SaaS, cuentas de cloud).
- **Gestión de parches y actualizaciones:** Automatiza el parcheo de sistemas operativos, aplicaciones y librerías en pipelines CI/CD.
- **Cifrado de datos:** Protege datos en reposo y en tránsito (TLS en APIs, discos cifrados en laptops).
- **Segmentación de redes:** Aísla entornos dev, test y prod para reducir el radio de impacto de un ataque.

Este paso es especialmente crítico en proveedores TI y MSPs que manejan infraestructuras multicliente. Un error de configuración aquí puede abrir la puerta a ataques en cadena.

## Gestión de flota de dispositivos con herramientas simples

Con equipos trabajando desde cualquier lugar y un arsenal de laptops, móviles y tablets en circulación, necesitas saber exactamente quién tiene qué y dónde está. Un inventario manual ya no basta: usar herramientas MDM/UEM simplifica la gestión de la flota y asegura que todos los endpoints cumplan las políticas.

### Puntos clave para una gestión eficiente:

- **Inventario en tiempo real:** Monitorea todos los dispositivos (laptops, móviles, IoT) con información sobre usuarios asignados y estado de cumplimiento.
- **Aplicación de políticas de seguridad:** Desde forzar actualizaciones y bloquear cámaras hasta impedir la instalación de apps no autorizadas.
- **Acciones remotas:** Bloqueo, borrado de datos y localización de dispositivos en caso de pérdida o robo.
- **Ejemplo de herramienta:** Con **Prey**, puedes asignar dispositivos a usuarios, configurar alertas automáticas (geofencing, batería baja, cambios de hardware) y mantener un historial de acciones ejecutadas para auditorías.

### Puntos clave para una gestión eficiente:

Hoy pensar que basta con un antivirus y una VPN es como creer que un paraguas lleno de agujeros te va a salvar de mojarte bajo un huracán. En el sector TI, donde cada laptop puede ser un vector y cada API una puerta trasera, necesitas un stack de seguridad que cubra todos los frentes: endpoints, identidades, redes y datos.

Además, recuerda que el **DBIR 2025** trae datos que quitan el sueño: el **44% de las brechas** involucran ransomware, y el **22% arrancan por endpoints sin visibilidad ni control.** Aquí te mostramos el "mínimo viable" para proteger tu operación y pasar cualquier auditoría ANCI sin sudar frío:

| Categoría | Descripción de la herramienta | Por qué importa | Ejemplos |
|---|---|---|---|
| **MDM (monitoreo de dispositivos)** | Monitorea laptops y móviles, aplica políticas, rastrea, bloquea o borra datos de forma remota. | El **22% de las brechas** arrancó por endpoints sin visibilidad ni control (DBIR 2025). | Prey , Microsoft Intune, Jamf Pro |
| **Gestión de parches** | Automatiza actualizaciones de SO, apps y contenedores; prioriza CVEs críticos. | El **20% de incidentes** explotó vulnerabilidades sin parchear. | Automox, Ivanti Neurons, WSUS |
| **Protección de endpoints (AV + EDR)** | AV detiene malware conocido; EDR detecta comportamientos raros y aisla hosts comprometidos. | El ransomware está en **44%** de las brechas; necesitas detección y respuesta en tiempo real. | SentinelOne, CrowdStrike Falcon |
| **SIEM / UEBA** | Centraliza logs, correla eventos y detecta anomalías antes de que escalen. | El **60% de los ataques** incluyen factor humano. | Splunk, Microsoft Sentinel, IBM QRadar |
| **Backups 3-2-1** | Copias locales y cloud, pruebas de restauración, con inmutabilidad o air-gap. | Sin copias íntegras no hay rescate; ransomware ahora apunta también a backups. | Veeam Backup, Acronis Cyber Protect |
| **Gestor de contraseñas** | Almacena contraseñas cifradas y genera claves fuertes. | Credenciales comprometidas son la puerta en **22% de las brechas.** | Bitwarden, 1Password, Keeper |
| **IAM / CABS** | Administra identidades, SSO y MFA; controla accesos según rol o contexto. | Principio de mínimo privilegio: que cada ingeniero use solo el acceso que necesita. | Okta, Azure AD PIM, ForgeRock |
| **Firewall perimetral / cloud** | Filtra tráfico, aplica reglas Zero Trust y protege entornos híbridos. | VPNs sin parchear fueron punto de entrada en **22% de incidentes** según DBIR. | Palo Alto Networks, Zscaler |

## Herramientas complementarias para nivel experto

Más allá del stack básico, estas soluciones son el “plus” que separa a un equipo de TI reactivo de uno proactivo:

| Categoría | Descripción de la herramienta | Qué cubre | Ejemplos |
|---|---|---|---|
| **IDS/IPS** | Monitoriza tráfico de red y bloquea ataques conocidos o patrones sospechosos en tiempo real. | Vulnerabilidades no parcheadas (+20% YoY). IDS alerta; IPS actúa. | Snort, Suricata, Cisco Secure IPS |
| **Análisis de vulnerabilidades** | Escanea hosts, apps y contenedores; prioriza riesgos y sugiere remediación. | El DBIR reporta **34% más exploits** este año. | Nessus Expert, Rapid7 InsightVM |
| **Concientización & phishing sim** | E-learning, micro-learning y campañas de phishing controladas para entrenar equipos. | Usuarios = 60% de las brechas. Entrena y mide la mejora. | KnowBe4, Hook Security, Phished |
| **Automatización de compliance** | Mapea controles ISO 27001/ NIST/Ley 21.663, genera reportes de auditoría automáticos. | ANCI exige evidencia clara. Centraliza datos y acelera revisiones. | Vanta, Hackmetrix, Drata, Tugboat Logic |

### Escenario realista para equipos de TI

1. **Prioriza según impacto:** Evalúa qué herramientas cubren los activos más críticos (infraestructura cloud, endpoints remotos).
2. **Integra telemetría:** Conecta MDM → SIEM → SOAR para correlacionar eventos y automatizar respuestas.
3. **Prueba tu plan B**: Simula restauración de backups, dispara playbooks de contención y mide tiempos de detección.

> Tip pro: Documenta cada paso. ANCI pedirá evidencias y tus futuros tú te lo agradecerán.


# 06

# Buenas prácticas de ciberseguridad en entornos TI

# Buenas prácticas de ciberseguridad en entornos TI

La ciberseguridad no es solo herramientas, es cultura y procesos. En entornos TI, donde el código, las credenciales y los endpoints se mueven a toda velocidad, adoptar buenas prácticas es lo que marca la diferencia entre contener un incidente y salir en los titulares. Aquí tienes cinco claves para fortalecer tu operación y cumplir con la Ley 21.663 sin perder agilidad.

### “Shift-left” en desarrollo: Seguridad desde el backlog

Integrar la seguridad desde el inicio del ciclo de desarrollo evita costosos parches posteriores. Incluye revisiones de código, análisis SAST y gestión de dependencias en la fase de planificación. En entornos DevOps, esto significa hacer de la seguridad una historia más en tu backlog y no un parche de última hora en producción.

### Política de Zero Trust segmentando entornos dev, test y prod

Adopta un enfoque Zero Trust que trate cada solicitud de acceso como potencialmente maliciosa. Segmenta entornos dev, test y prod para evitar que un fallo en uno comprometa a los otros. Esto limita el movimiento lateral de atacantes y mejora la contención de incidentes en infraestructuras multitenant y pipelines CI/CD.

### Rotación y revisión de secretos en pipelines y contenedores

Los secretos (claves API, tokens, passwords) en pipelines y contenedores son oro para los atacantes. Configura políticas de rotación periódica y automatiza su gestión con herramientas como HashiCorp Vault o AWS Secrets Manager. Audita regularmente repositorios para asegurarte de que no se filtren secretos hardcodeados.

### Teletrabajo seguro: VPN con split-tunneling controlado + MDM obligatorio

Con equipos distribuidos, el teletrabajo seguro es clave. Usa VPNs con split-tunneling controlado para priorizar tráfico crítico y evitar cuellos de botella. Complementa con un MDM que permita aplicar políticas de seguridad y localizar o borrar dispositivos en caso de pérdida o robo. Aun en entornos no remotos, estas políticas son invaluables, ya que hoy día está normalizado el uso de dispositivos personales para uso laboral.

### Gestión de vulnerabilidades con ciclos ≤30 días para CVE críticas

Un ciclo de parcheo ágil es vital. Apunta a cerrar CVEs críticas en 30 días o menos para reducir la ventana de exposición. Automatiza escaneos con soluciones como Nessus o Qualys y prioriza remediaciones según el riesgo e impacto en servicios críticos. Esto es esencial en infraestructuras TI dinámicas donde las configuraciones cambian constantemente.

### El delegado de ciberseguridad en empresas TI

En el sector TI, el delegado o encargado de ciberseguridad no es un mero requisito de la Ley 21.663: es el guardián del negocio. Este rol combina conocimientos técnicos con habilidades de gestión para mantener la operación segura y en regla. Desde dialogar con la ANCI hasta guiar auditorías internas, aquí está lo que debe aportar este perfil clave.

### Alinea los KPIs de seguridad con roadmap de producto y SLA de clientes

En empresas TI, el delegado debe asegurar que los objetivos de seguridad no chocan con los plazos de desarrollo o las expectativas de los clientes. Su trabajo es balancear protección y agilidad, alineando controles con el roadmap de producto y garantizando que los SLA de ciberseguridad sean realistas y cumplibles.

### Debe entender redes, cloud y ciclo de vida de software

Un delegado en una empresa TI no puede quedarse solo en lo básico. Necesita conocimientos sólidos sobre redes corporativas, infraestructuras cloud (AWS, Azure, GCP) y el ciclo de vida de software. Esto le permite identificar riesgos en cada fase, desde el desarrollo hasta la operación, y establecer controles que se adapten a entornos DevOps y multitenant.

### Puede ser un CISO interno, un vCISO externo o un rol híbrido con autoridad presupuestaria

Dependiendo del tamaño y madurez de la organización, el delegado puede ser un CISO de planta, un CISO virtual contratado o un rol híbrido que combine gestión con apoyo técnico. Lo importante es que tenga suficiente autoridad presupuestaria para tomar decisiones y responder rápido ante incidentes o auditorías regulatorias.

### Interlocutor principal ante ANCI y CSIRT; prepara reportes y auditorías

Este rol será la cara visible de tu empresa frente a la Agencia Nacional de Ciberseguridad y el CSIRT Nacional. Es quien coordina con su equipo la gestión y notificación de incidentes, entrega evidencia durante auditorías y lidera el cumplimiento de los plazos (como el reporte en 3 horas tras un ataque significativo). También debe saber traducir lenguaje técnico en informes claros para reguladores.

### En PYMEs: cómo cubrir el rol sin romper el presupuesto

Para PYMEs TI, contratar un CISO full-time puede ser inviable. En estos casos, un vCISO o un proveedor de servicios gestionados de ciberseguridad (MSSP) puede asumir el rol. También pueden designar a un responsable interno con formación básica reforzada por consultoría externa. Lo clave es que haya alguien que lidere la estrategia y actúe como punto de contacto con la ANCI.

07


# Cómo Prey puede ayudarte a cumplir con la Ley 21.663

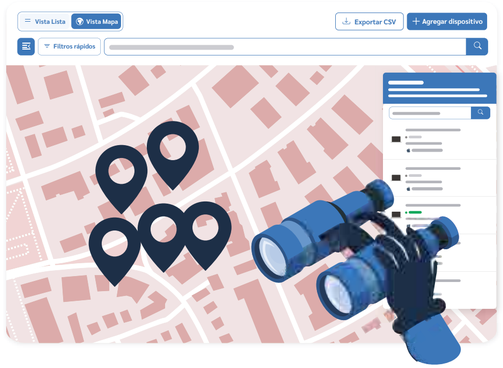
# Cómo Prey puede ayudarte a cumplir con la Ley 21.663

Prey es la navaja suiza para empresas TI que buscan cumplir con la Ley 21.663 sin montar un stack de seguridad monstruoso. Su plataforma unifica la gestión, protección y monitoreo de dispositivos, ofreciendo control sobre activos críticos, una respuesta rápida ante incidentes y la trazabilidad que un auditor de la ANCI te pedirá, todo desde una consola limpia y accesible.

## Detección de incidentes y reacción rápida


Con funciones como geofencing, alertas automáticas y detección de comportamientos inusuales (ej. cambios de usuario o hardware), Prey actúa como un sistema de alerta temprana. Además, permite ejecutar acciones remotas: bloquear pantallas, activar alarmas o enviar mensajes al usuario. Esto acelera la contención de incidentes como laptops comprometidas o endpoints perdidos en entornos remotos.

## Visibilidad y control de tu flota




Prey te da una vista 360° de todos los dispositivos en tu organización: laptops de desarrolladores, móviles de soporte y hasta tablets en entornos de testing. Desde su panel centralizado puedes geolocalizar equipos, aplicar etiquetas y filtros (por área, cliente o proyecto) y gestionar múltiples sistemas operativos (Windows, macOS, ChromeOS, Android, Ubuntu). Ideal para MSPs y SaaS con flotas híbridas o equipos distribuidos.

## Protección de datos en caso de pérdida o robo


Cuando un dispositivo crítico cae en manos equivocadas, cada segundo cuenta. Prey ofrece herramientas como Remote Wipe, Factory Reset y cifrado remoto con BitLocker en Windows para eliminar datos sensibles o inutilizar equipos robados. Esto no solo protege la información, sino que ayuda a cumplir con la obligación legal de salvaguarda de datos y notificación a la ANCI.

## Evidencia y trazabilidad para auditorías


La plataforma registra cada movimiento: cambios de configuración, ubicación de dispositivos y ejecuciones remotas, todo consolidado en su Audit Log. Este historial detallado es oro durante auditorías de la ANCI o revisiones internas, permitiéndote demostrar cumplimiento con la Ley 21.663 y estándares como ISO 27001.

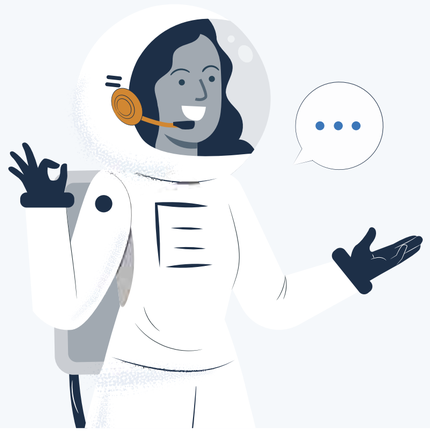
## Apoyo para instituciones con bajo presupuesto


Para PYMEs tecnológicas o startups sin presupuesto para un SGSI completo, Prey cubre muchos de los controles básicos exigidos por la ley: inventario, monitoreo, protección de endpoints, trazabilidad y respuesta rápida. Todo en una plataforma intuitiva y multi-plataforma, sin necesidad de sobredimensionar tu stack ni tu equipo.

## Monitoreo de brechas y credenciales en la Dark Web


¿Y si las credenciales de tu equipo aparecen en foros de la dark web? Con Prey, puedes saberlo antes que los atacantes. Su servicio de monitoreo te alerta sobre filtraciones de correos y contraseñas corporativas, permitiéndote rotar credenciales de inmediato y evitar accesos no autorizados. En empresas TI, esto es especialmente crítico por la cantidad de accesos privilegiados que gestionan.

## ¿Quieres ver cómo Prey puede ayudarte con el cumplimiento?



Si quieres conocer de primera mano cómo Prey puede fortalecer tu estrategia de ciberseguridad y apoyar el cumplimiento de la Ley 21.663, HIPAA, FERPA y otras normativas, te invitamos a agendar un

Solicita un demo guiada o escríbenos a sales@preyproject.com para conocer tu caso.

# Sobre Prey

Es una herramienta multi-plataforma para el **Rastreo y la Seguridad** de tus dispositivos remotos.  Es un servicio que actualmente protege más de 8 millones de equipos y sus datos cada día, alrededor de todo el mundo.

Prey comenzó en 2009 como una pequeña compañía de tecnología que se propuso un solo objetivo: ayudar a las personas a mantener el control de sus dispositivos. 15 años más tarde, nuestro servicio ha evolucionado hasta convertirse en una confiable multi herramienta para personas y negocios. Somos expertos en localizar, proteger y administrar tus dispositivos tecnológicos para el ocio y el trabajo. Y un equipo de personas orgullosas de poder ofrecerte apoyo.

Prey para: **Personas** | **Organizaciones** | **Escuelas y Universidades**