Guía de cumplimiento

ley 21.663

para el sector educativo

Prey Inc.

¿Por qué la educación está en la mira?

La digitalización del entorno escolar llegó para quedarse: clases online, plataformas educativas, sistemas de gestión académica y una flota de dispositivos que van de mano en mano entre alumnos y docentes. Pero con cada avance tecnológico, también llegan nuevos riesgos.

Un ejemplo claro fue el ataque de **ransomware a la Universidad Técnica Federico Santa María** en 2024, que dejó expuestos datos críticos y paralizó servicios educativos. Situaciones como esta no solo comprometen evaluaciones o calendarios académicos; también ponen en jaque la información personal de estudiantes, docentes y administrativos, desde datos de contacto hasta historiales médicos y financieros.

En este contexto, la Ley 21.663 de Chile marca un antes y un después. Esta normativa establece los principios, obligaciones y mecanismos para que los operadores de servicios esenciales (OSE) adopten una postura activa en ciberseguridad. Desde implementar sistemas SGSI hasta reportar incidentes críticos en pocas horas, la ley busca garantizar la continuidad de servicios clave y la protección de datos en sectores estratégicos.

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 institución debe cumplir con la ley?

¿Mi institución debe cumplir con la ley?

Aunque hoy colegios, liceos, universidades y centros de formación técnica no están expresamente calificados como Operadores de Servicios Esenciales (OSE), pero eso no significa que estén fuera de riesgo ni que puedan ignorar la normativa.
La Agencia Nacional de Ciberseguridad (ANCI) puede ampliar esta clasificación mediante resolución fundada, incorporando a instituciones públicas y privadas cuya interrupción, afectación o ataque pueda causar un daño grave al funcionamiento social, económico o estatal.

No obstante, el sector educativo es bien variado y existen ciertas excepciones donde si aplica como OSE:

¿Cuándo una institución educativa podría ser considerada OSE o estar sujeta a la ley?

- **Si forma parte de la administración central del Estado** (por ejemplo, ministerios o servicios públicos con funciones educativas).
- **Si gestiona infraestructura crítica digital o plataformas nacionales clave** (como REUNA, bibliotecas digitales o sistemas de evaluación).
- **Si es parte de un Servicio Local de Educación Pública (SLEP)** u otra entidad con dependencia directa del Ministerio de Educación.
- **Si operan clínicas asistenciales**, este tipo de universidades tienen un rol doble: educacional y asistencial. En estos casos, es muy probable que sus infraestructuras tecnológicas y de atención médica se consideren críticas
- **Si trabajas como proveedores EdTech** , la cadena de suministro también puede generar responsabilidades.

Si respondiste “sí” a una o más de estas preguntas, tu institución podría ser clasificada como Operador de Servicios Esenciales (OSE) por la ANCI y quedar obligada a cumplir con los requisitos de la ley a partir de junio de 2025. Ahora es el momento ideal para prepararse y no ser tomado por sorpresa.

¿Y si no soy OSE?
Aunque tu institución no esté obligada a cumplir todos los artículos de la Ley 21.663, no significa que no debas prepararte.

El llamado desde la ANCI es claro:

Todas las instituciones educativas públicas o privadas, esenciales o no, deberían al menos:

- **Adoptar buenas prácticas básicas de ciberseguridad.** Esto incluye contar con inventario de activos, monitoreo, control de accesos, protección de endpoints y planes de respuesta a incidentes.
- **Reportar incidentes relevantes.** Si ocurre una filtración de datos de estudiantes, un ataque de ransomware o un acceso no autorizado, es recomendable (y responsable) notificar a la ANCI para evitar su propagación y mejorar la respuesta nacional.

02 Riesgos digitales específicos del entorno educativo

Riesgos digitales específicos del entorno educativo

En el contexto actual, donde muchos alumnos y docentes trabajan tanto desde casa o fuera del aula, los riesgos se amplifican. El entorno educativo demanda una visión integral de seguridad que abarque conexiones remotas, redes institucionales y dispositivos personales.

Dentro de los riesgos asociados al sector educativo tenemos:

Robo o pérdida de dispositivos con información sensible

Imagina un notebook con evaluaciones, calificaciones o datos de apoderados extraviado en el transporte público: todo ese contenido queda expuesto. Esa información no solo se pierde sino que puede terminar en manos equivocadas, afectando la privacidad de estudiantes y la credibilidad de la institución.

Accesos indebidos a plataformas internas

Cuando las plataformas académicas no tienen controles robustos de acceso, cualquier persona con credenciales débiles o robadas puede colarse dentro. En Chile han ocurrido ataques de ransomware a universidades, como el caso de la USM en 2024, que paralizaron sistemas clave y pusieron en riesgo datos de toda la comunidad educativa.

Phishing a estudiantes, docentes o staff administrativo

Los correos mimetizados y enlaces falsos son trampas habituales. Un docente o alguien del staff administrativo que ingresa sus credenciales en un sitio malicioso abre la puerta a atacantes, comprometiendo cuentas y provocando brechas o filtraciones. El phishing es una amenaza silenciosa pero masiva.

Uso inadecuado de redes por parte de terceros

Cuando visitantes, apoderados o alumnos usan redes Wi-Fi escolares sin supervisión, pueden activar malware que se propaga a otros dispositivos. Este tipo de acceso informal genera una entrada no controlada a los sistemas institucionales.

Brechas por dispositivos personales (BYOD, celulares en sala, etc.) El uso de celulares o laptops propias en el aula facilita el aprendizaje, pero representa un vector de riesgo: si no están debidamente protegidos, pueden cargar virus, aplicaciones no autorizadas o permitir conexiones inseguras. Un solo dispositivo comprometido puede afectar la seguridad global de la red.

03 Obligaciones principales según la ley

Obligaciones principales según la ley

La Ley 21.663 establece un conjunto de obligaciones (artículo 8) diseñadas para que las organizaciones críticas puedan prevenir, detectar y responder a incidentes de ciberseguridad. También obliga a reportar al CSIRT nacional aquellos incidentes con efectos significativos en sus operaciones.

Como ya mencionamos antes, aunque las medidas se dirigen principalmente a los Operadores de Servicios Esenciales (OSE) y Operadores de Importancia Vital (OIV), instituciones educativas que gestionan grandes volúmenes de datos o que dependen de plataformas digitales podrían ser incluidas en estas categorías por la ANCI si un ataque compromete su funcionamiento o impacta a la comunidad escolar.

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 colegios y universidades, esto significa el primer paso para que la Agencia pueda coordinar acciones, supervisar su ciberseguridad y notificarles sobre protocolos aplicables. Un registro actualizado es clave para demostrar la disposición institucional a cumplir con la normativa.

Desde el 11 de junio del 2025 ya se encuentra abierto las inscripciones en el portal ANCI:
portal ANCI:

Designación de delegado de ciberseguridad

OSE : ✓ | OIV: ✓

El delegado de ciberseguridad será el punto de contacto con la ANCI. En entornos educativos, este rol puede recaer en el jefe de TI o en un profesional externo con experiencia en seguridad escolar, encargado de coordinar acciones, informar a la dirección y liderar la respuesta ante incidentes como filtraciones de datos de alumnos o ataques de ransomware.

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 integre políticas y procesos vivos, no meras carpetas de documentos. En instituciones educativas implicadas significa gestionar riesgos sobre plataformas de notas, redes Wi-Fi y dispositivos compartidos, asegurando la continuidad educativa aun durante incidentes.

Aprende cómo aplicar un SGSI en educación:
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 el sistema de matrículas o correos masivos de phishing— 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: ✓

Se deben realizar auditorías y simulacros de ciberataques. Para centros educativos catalogados como OIV, esto puede incluir prácticas sobre cómo responder a un robo de notebooks con datos de alumnos o a un ataque que comprometa el correo institucional o el sistema computacional interno.

Planes de continuidad operacional y ciberseguridad

OSE : ✗ | OIV: ✓

Un plan de continuidad bien diseñado permite a la institución educativa mantener clases y servicios online operativos incluso durante una crisis cibernética. La ley exige revisarlos cada dos años.

Recomendamos:
Crea tu plan de respuesta a incidentes de ciberseguridad

Medidas para reducir impacto y propagación

OSE : ✗ | OIV: ✓

En caso de incidentes, las instituciones deben actuar rápido: desconectar equipos comprometidos, bloquear cuentas afectadas o aislar redes escolares para evitar daños mayores.

Certificaciones según el artículo 28

OSE : ✗ | OIV: ✓

Se exige certificación como ISO 27001 para demostrar que el SGSI y los planes de continuidad funcionan. Aunque no obligatorio para OSE, se recomienda adoptar controles basados en ISO/NIST para colegios y universidades que gestionan datos de menores.

Notificación a potenciales afectados

OSE : ✗ | OIV: ✓

Si un ciberataque compromete información sensible (como listas de alumnos o datos de apoderados), la institución debe notificar a los afectados cuando sea posible identificarlos.

Programas de capacitación y campañas de ciberhigiene

OSE : ✗ | OIV: ✓

Capacitar a docentes, administrativos y estudiantes es clave para evitar incidentes por errores humanos. Estas campañas pueden enseñar desde reconocer correos de phishing hasta buenas prácticas con dispositivos escolares compartidos.

Cumplimiento de normativas técnicas ANCI o sectoriales

OSE : ✓ | OIV: ✓

Las instituciones deben adoptar estándares técnicos (ISO 27001, NIST, CIS Controls) dictados por ANCI o su regulador sectorial. Esto asegura que sus sistemas y procesos estén alineados con las mejores prácticas y preparados para auditorías.

Recursos adicionales:
Checklist descargable: Descubre cómo simplificar el cumplimiento paso a paso para instituciones educativas.

04

Qué pasa si no cumples

Qué pasa si no cumples

La Ley marco clasifica las infracciones en tres niveles: leves, graves y gravísimas. Cada categoría depende de la naturaleza y el impacto del incumplimiento. Las leves incluyen retrasos en la entrega de información no crítica; las graves abarcan la falta de implementación de estándares o la omisión de reportes obligatorios; y las gravísimas son las más severas, asociadas a incidentes de alto impacto o reincidencias.

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, omisión de reportes críticos, obstaculización.	10.000 UTM	20.000 UTM
Gravísima	Reincidencia en infracciones graves o incidentes con impacto significativo.	20.000 UTM	40.000 UTM

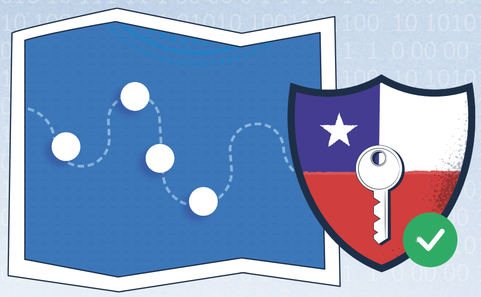
Tipos de infracciones según el artículo 38

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

Los factores agravantes pueden elevar las sanciones impuestas. La reincidencia, el impacto económico o social del incumplimiento y el tamaño de la empresa son elementos que la ANCI considera al determinar la multa. Las organizaciones de mayor relevancia estratégica enfrentan sanciones más altas si no toman medidas para mitigar riesgos.

Por ejemplo, un OIV que no informa un ciberataque a potenciales afectados comete una infracción grave. Si además no toma acciones para contener la amenaza y el incidente afecta servicios esenciales, la falta puede escalar a gravísima, con multas millonarias y posibles inhabilitaciones operativas.

05



Pasos prácticos para cumplir con la Ley 21.663

Pasos prácticos para cumplir con la Ley 21.663

Esta sección puedes verla como una hoja de ruta con los pasos clave para implementar un SGSI, adoptar las herramientas correctas y preparar a tu comunidad educativa para los retos que plantea la Ley 21.663.

Sigue esta guía para avanzar con confianza y asegúrate de que tu colegio, liceo, universidad o centro de formación técnica esté listo para cualquier incidente que pueda afectar su funcionamiento. ¿Listo para ponerte manos a la obra?

Diagnóstico inicial

Antes de lanzarte a implementar controles o adquirir soluciones de seguridad, necesitas saber dónde estás parado. El diagnóstico inicial es como un chequeo general para tu institución: identifica activos críticos, evalúa riesgos y detecta brechas en tus procesos actuales.

Este paso te dará una visión completa de tus puntos fuertes y de las áreas que requieren atención para cumplir con la Ley 21.663. En el caso de colegios, liceos, instituciones de investigación y universidades, este diagnóstico también ayuda a proteger datos sensibles de alumnos, docentes y apoderados, así como a garantizar la continuidad de clases y servicios digitales.

Pasos del diagnóstico inicial:

Inventario de activos: Haz un inventario completo de todos los activos de información: notebooks y tablets en préstamo a estudiantes, servidores que alojan plataformas educativas, redes Wi-Fi del campus, sistemas de gestión académica y datos sensibles como historiales de notas o información de salud de alumnos. Este paso es esencial para saber qué necesitas proteger y para identificar qué tan expuesto está tu entorno actual frente a posibles amenazas.

Análisis de riesgos: Realiza un análisis detallado de las amenazas que podrían afectar tu operación. Considera vulnerabilidades internas (como contraseñas débiles en cuentas de docentes) y externas (ransomware que podría bloquear sistemas de matrícula online). Evalúa la probabilidad de que ocurran incidentes y el impacto sobre servicios educativos, reputación institucional y la seguridad de la comunidad escolar. Esta información te ayudará a priorizar las acciones más críticas.

Revisión de políticas actuales: Examina si ya existen políticas o procedimientos sobre seguridad de la información en tu institución. Pregúntate: ¿cubren riesgos como el uso de dispositivos personales (BYOD) en el aula o la protección de plataformas de e-learning? ¿Están alineadas con estándares como ISO 27001? Este análisis permite identificar vacíos normativos y ajustar la gobernanza antes de implementar un SGSI.

Mapeo de procesos: Identifica cómo se mueve la información dentro de la institución: ¿quién accede a las bases de datos de alumnos?, ¿cómo se gestionan las credenciales para aulas virtuales?, ¿dónde podrían existir puntos débiles? Visualizar estos flujos permite detectar procesos que requieren controles adicionales para asegurar la integridad y confidencialidad de los datos.

Reporte de brechas: Elabora un informe claro con las brechas y vulnerabilidades detectadas en los pasos anteriores. Por ejemplo, la falta de cifrado en notebooks que llevan los estudiantes a casa o redes Wi-Fi abiertas en sectores del campus. Prioriza las áreas críticas según el riesgo e impacto potencial. Este documento será la base para tu plan de acción y te permitirá justificar ante la dirección la necesidad de invertir en seguridad.

Recursos adicionales para el sector educativo:

- Cómo implementar un programa de gestión de riesgos en colegios y universidades
- Matriz de riesgos: Guía para líderes de TI en educación

Designación del delegado

Una vez que sabes dónde estás, es hora de nombrar a la persona que liderará el cambio. La ley exige como mínimo un delegado de ciberseguridad como enlace con la ANCI, y en instituciones educativas este rol podría ser asumido por el jefe de TI o en instituciones pequeñas por un docente con experiencia en tecnologías, apoyado por un equipo externo si es necesario.

En universidades grandes o redes de colegios, se recomienda tener un encargado de ciberseguridad y un equipo de apoyo que se encargue de toda la gestión y la notificación de incidentes. Este rol será clave para coordinar acciones, monitorear avances y garantizar que el SGSI se mantenga activo y actualizado en un entorno donde los riesgos van desde el uso de plataformas de e-learning hasta la gestión de dispositivos compartidos.

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

Elegir un marco de referencia sólido es un paso crucial para estructurar tu SGSI y cumplir con la Ley 21.663. Aunque existen varios, como NIST CSF, recomendamos ISO 27001 porque es el estándar en el que se basa la normativa chilena y es ampliamente usado en instituciones educativas a nivel mundial.

Además, facilita auditorías y certificaciones internacionales, algo especialmente útil para universidades que colaboran en redes globales de investigación o programas de intercambio. NIST puede ser un buen complemento para áreas muy técnicas, como departamentos de TI en universidades o centros de investigación.

Aspecto	ISO 27001	NIST Cybersecurity Framework
Enfoque	Sistema de gestión completo basado en ciclo PDCA.	Guía flexible de buenas prácticas para gestión de riesgos.
Certificación	Certificable a nivel internacional.	No certificable, es una guía voluntaria.
Alineación con Ley 21.663	Totalmente alineado, citado como referencia principal.	Complementa, pero no reemplaza ISO.
Cobertura geográfica	Reconocido globalmente, útil para instituciones con convenios internacionales.	Predominante en EE. UU. y sectores técnicos.
Uso ideal	Escuelas y universidades que buscan un SGSI estructurado y certificable.	Departamentos TI que necesitan guías rápidas y flexibles.

Automatización de alertas y trazabilidad

En el entorno educativo, donde múltiples usuarios (docentes, alumnos, administrativos) interactúan diariamente con plataformas y dispositivos, el tiempo de reacción lo es todo. Automatizar alertas permite detectar y responder a incidentes en tiempo real, sin depender de que “alguien se dé cuenta a tiempo”.

Por otro lado, la trazabilidad es crítica: la Ley 21.663 exige registros detallados para demostrar acciones y decisiones en auditorías, algo especialmente relevante cuando se gestionan datos de menores o información académica sensible. Ambas prácticas juntas te dan control y tranquilidad para mantener la continuidad educativa.

Elemento	¿Qué es?	¿Qué ofrece?	¿Qué aporta?	Cómo y con qué app
Automatización de alerta	Un sistema que genera notificaciones automáticas cuando detecta comportamientos anómalos o incidentes, como accesos no autorizados o cambios en configuraciones críticas.	Alertas en tiempo real por email, SMS o dashboards para que el equipo de TI actúe sin demoras.	Reduce tiempos de respuesta y mitiga el impacto de ataques antes de que escalen.	Herramientas tipo SIEM (Splunk, Graylog) para alertas avanzadas. Con Prey, puedes configurar reglas automáticas (geofencing, batería baja, cambios de hardware) para recibir notificaciones instantáneas y aplicar acciones remotas como bloqueo o borrado en dispositivos escolares.
Trazabilidad	El registro continuo y detallado de todas las actividades relacionadas con la seguridad de la información, desde inicios de sesión hasta cambios en permisos.	Logs de auditoría completos con fechas, responsables y acciones tomadas, alineados con la Ley 21.663.	Facilita auditorías, demuestra cumplimiento y ayuda a reconstruir eventos tras incidentes.	Plataformas como Vanta o Drata centralizan logs y generan reportes de cumplimiento. En entornos educativos, Prey mantiene un historial de acciones ejecutadas (bloqueos, recuperaciones, cambios de configuración) para aportar evidencia clara en auditorías y ante solicitudes de la ANCI.

Capacitación y concientización interna

Puedes tener el mejor firewall del mundo, pero si alguien en la institución abre un archivo adjunto sospechoso, el castillo se viene abajo. La formación continua del eslabón más débil no es opcional: es tu mejor defensa contra errores humanos, que el DBIR 2025 identifica como causa en el 60% de las brechas. Un equipo bien entrenado es un escudo activo contra amenazas.

Ideas y plataformas para capacitar a tu equipo

- **Simulaciones de phishing**
  Crea campañas falsas de phishing para entrenar al personal en la detección de correos fraudulentos.

  Plataforma recomendada: KnowBe4, Proofpoint Security Awareness.

- **Cursos interactivos de ciberseguridad**
  Ofrece módulos cortos y dinámicos sobre prácticas de higiene digital, uso seguro de contraseñas y manejo de datos sensibles.

  Plataforma recomendada: Udemy for Business, Coursera.

- **Cartelería digital y recordatorios**
  Usa screensavers, emails o apps internas para reforzar mensajes clave (no compartir contraseñas, cuidado con USB desconocidos, etc.).

  Plataforma recomendada: herramientas internas de comunicación como Slack.

- **Simulacros de incidentes**
  Realiza ejercicios prácticos donde los equipos respondan a un ciberataque simulado, desde el reporte hasta la contención.

  Plataforma recomendada: Cyberbit, RangeForce.

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

Cuando algo falla —y en un entorno educativo con miles de usuarios y dispositivos conectados, tarde o temprano sucederá— lo importante no es solo evitarlo, sino saber cómo reaccionar. La **Ley 21.663** exige a las organizaciones tener un **PCO** para garantizar que los servicios esenciales sigan funcionando tras un ciberataque.

Para universidades o colegios, esto puede significar mantener operativas las plataformas de clases online, los sistemas de matrícula o incluso la red Wi-Fi del campus durante una crisis. Aquí te conviene mirar el **ISO 22301**, el estándar de referencia en continuidad de negocio, que puede integrarse fácilmente con ISO 27001.

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

- **Identificación de procesos críticos:** Define qué operaciones no pueden detenerse bajo ninguna circunstancia, como el acceso a plataformas de aprendizaje o los sistemas de pago escolar, y los recursos necesarios para mantenerlas activas.
- **Evaluación de riesgos y análisis de impacto:** Analiza escenarios de fallas (ransomware que bloquea el correo institucional o pérdida de laptops con datos sensibles) y su efecto en el servicio educativo. Prioriza áreas que requieren planes robustos.
- **Protocolos de respuesta rápida:** Establece pasos claros para contener, mitigar y notificar incidentes, incluyendo reportes a la ANCI en menos de 3 horas cuando los datos de estudiantes o docentes estén comprometidos.
- **Roles y responsabilidades:** Asigna quién hace qué durante una crisis, desde el área TI que bloquea dispositivos hasta la dirección que comunica a la comunidad educativa.
- **Pruebas y simulacros periódicos:** Ensaya los planes regularmente con docentes y personal administrativo para asegurarte de que todos sepan cómo actuar ante un incidente.
- **Planes de recuperación y retorno a la normalidad:** Diseña cómo restaurar clases online, sistemas académicos y redes tras la contención del incidente.
- **Etapa de lecciones aprendidas y re-evaluación:** Tras un incidente, documenta qué salió bien y qué se puede mejorar. Esto es especialmente útil para centros educativos con rotación frecuente de personal o estudiantes.

Pruebas, simulacros y auditorías

Tener un plan suena bien, pero ¿funciona cuando las cosas se ponen feas? Las pruebas, simulacros y auditorías son la única forma de asegurarte de que tus controles y procesos no fallarán cuando realmente los necesites.

Además, la **Ley 21.663** exige revisiones periódicas (mínimo cada dos años) para mantener todo afinado y listo. En el sector educativo, un simulacro podría incluir la pérdida simulada de datos de un servidor de notas o un ataque de denegación de servicio a la red escolar.

Elemento	¿Qué es?	¿Qué aporta?	¿Qué involucra?
Pruebas	Ejecuciones controladas de sistemas y procesos para comprobar su funcionamiento.	Identifica fallos técnicos o de configuración antes de un incidente real.	Revisar backups de plataformas educativas, probar restauración de datos de alumnos, verificar que alertas se disparen correctamente.
Simulacros	Ejercicios prácticos donde se simula un incidente de seguridad para evaluar la respuesta del equipo.	Entrena al personal y pone a prueba la coordinación y toma de decisiones bajo presión.	Escenarios como ransomware en la red de la biblioteca o filtración de datos de alumnos; roles definidos y tiempos cronometrados.
Auditorías	Evaluaciones formales y periódicas para revisar el cumplimiento de políticas y normativas.	Aporta evidencia para la ANCI y asegura alineación con estándares como ISO 27001 o 22301.	Auditorías internas y externas, revisión de registros, entrevistas con personal de TI y análisis de brechas en procesos escolares.

Plan de implementación por fases

Dentro del contexto educativo sabemos que intentar implementar un SGSI de golpe puede ser abrumador, costoso y poco realista. Por eso recomendamos dividirlo en fases pequeñas mas manejable en el tiempo. Este enfoque permite priorizar lo más crítico, gestionar recursos de forma eficiente y mostrar avances rápidos a la dirección. Además, facilita ajustes antes de una implementación total.

Aquí te damos un ejemplo de implementación por fases:

Fases	Nombre	Descripción
Fase 1	Diagnóstico y planificación	Realizar el diagnóstico inicial y definir el alcance del SGSI.
Fase 2	Políticas y procedimientos básicos	Redactar políticas de seguridad y establecer roles y responsabilidades.
Fase 3	Controles técnicos iniciales	Implementar controles esenciales inicialmente como control de accesos y backups, para luego trazar una ruta hacia controles más complejos pero necesarios.
Fase 4	Formación y concientización	Capacitar a los equipos en buenas prácticas de ciberseguridad.
Fase 5	Auditorías internas y ajustes	Probar el sistema, identificar brechas y hacer correcciones antes de la certificación o auditoría.

Documentación y evidencia

En ciberseguridad, lo que no está documentado “no existe” a los ojos de un auditor. La Ley 21.663 exige mantener registros claros y actualizados para demostrar que realmente aplicas las medidas de seguridad. Esta evidencia no solo es útil para cumplir, también te salva cuando necesitas reconstruir lo que pasó tras un incidente.

Documentación clave que deberías tener a mano

- **Políticas y procedimientos**
  - Política de seguridad de la información.
  - Procedimientos de gestión de incidentes.
  - Planes de continuidad operativa y recuperación de desastres.
- **Registros de actividades**
  - Logs de acceso a sistemas críticos.
  - Historial de configuraciones y cambios en la infraestructura.
  - Ejecuciones de acciones remotas (como bloqueos o borrados con Prey).
- **Evidencia de capacitación**
  - Listados de sesiones de formación realizadas.
  - Certificados de participación del personal.
  - Resultados de campañas de concientización (simulaciones de phishing, por ejemplo).
- **Informes de auditorías y simulacros**
  - Auditorías internas y externas completas.
  - Resultados y lecciones aprendidas de simulacros de ciberataques.
  - Planes de acción derivados de las auditorías.
- **Certificaciones y cumplimiento**
  - Certificados ISO 27001 o ISO 22301 (si los tienes).
  - Evidencia de revisiones periódicas según la Ley 21.663.
  - Reportes enviados a la ANCI o al CSIRT Nacional.
- **Inventario de dispositivos y quienes lo manejan**
  - Laptops y desktops corporativos.
  - Dispositivos móviles (smartphones y tablets).
  - Servidores locales y en la nube.
  - Equipos de red (routers, switches, firewalls físicos).
  - Dispositivos IoT críticos (cámaras de seguridad, sensores, etc.).
  - Medios de almacenamiento externo (discos duros, USBs, backups físicos).

Herramientas tecnológicas recomendadas

Hoy en día, pensar que basta con un antivirus y una VPN es como creer que con cerrar la puerta del colegio basta para detener a alguien con una copia de las llaves. En el entorno educativo, donde alumnos y docentes acceden desde múltiples dispositivos y redes —en clases presenciales, online o mixtas—, todos llevamos un pedazo del trabajo a casa (ese notebook con datos de alumnos o el móvil con acceso a la plataforma de notas). Por eso necesitas un stack de seguridad que cubra todos los frentes y te permita proteger tanto la infraestructura institucional como los dispositivos en préstamo.

En esta lista no solo encontrarás las herramientas clave que no pueden faltar en un SGSI, sino también datos recientes del Data Breach Investigation Report 2025 que demuestran por qué son críticas para no ser la próxima universidad o liceo en las noticias por una filtración de datos:

Categoría	Descripción de la herramienta	Por qué importa	Ejemplos
MDM (monitoreo de dispositivos)	Monitorea laptops y tablets en préstamo, aplica políticas de uso, rastrea, bloquea o borra datos de forma remota desde una consola.	El 22% de las brechas comenzaron en endpoints sin visibilidad ni control. En colegios, la pérdida de un notebook con datos de alumnos puede ser catastrófica.	Prey , Microsoft Intune, Jamf Pro
Gestión de parches	Automatiza actualizaciones de sistemas y apps en equipos escolares, prioriza CVEs críticos y verifica su instalación.	El 20% de los incidentes explotó vulnerabilidades sin parchear; un solo equipo desactualizado puede abrir toda la red educativa.	Automox, ManageEngine Patch Manager Plus, Ivanti Neurons, WSUS
Protección de endpoints (AV + EDR)	El antivirus detiene malware conocido; el EDR monitoriza comportamientos, aísla hosts y orquesta respuestas en tiempo real.	El 44% de las brechas incluyeron ransomware. Ideal para universidades con laboratorios de informática o redes abiertas.	Avast Business + CrowdStrike Falcon, SentinelOne
SIEM / UEBA	Centraliza logs de plataformas educativas, correlaciona eventos y aplica analítica para detectar anomalías antes de escalar.	El 60% de los ataques tienen factor humano; detectar accesos anómalos de cuentas docentes o administrativas es clave.	Splunk, IBM QRadar, Microsoft Sentinel
Backups 3-2-1	Crea copias locales y en la nube, prueba restauración y protege con inmutabilidad o air-gap.	Sin copias íntegras no hay rescate: ransomware en un servidor escolar puede dejar semanas sin clases online.	Veeam Backup & Replication, Acronis Cyber Protect
Gestor de contraseñas	Guarda contraseñas cifradas, genera claves fuertes y evita que docentes y alumnos reutilicen las mismas en varias cuentas.	Credenciales robadas fueron la puerta en el 22% de los casos.	Bitwarden , 1Password, Keeper Security
IAM / CABS	Administra identidades, gestiona SSO y MFA, aplica acceso granular basado en roles o contexto (estudiante, docente, TI).	Principio de mínimo privilegio: que cada usuario acceda solo a lo que necesita, evitando riesgos en plataformas escolares.	Okta, Azure AD PIM, ForgeRock
Firewall perimetral / cloud	Filtra y segmenta tráfico, aplica reglas Zero Trust y detiene exploits en tiempo real, incluso en entornos híbridos.	Appliances y VPNs sin parches son responsables del 22% de accesos iniciales; críticos en redes escolares abiertas.	Palo Alto Networks, Zscaler Zero Trust Exchange

Herramientas complementarias

Además del “stack básico” de seguridad, existen herramientas complementarias que llevan tu defensa al siguiente nivel. En el sector educativo, donde el volumen de usuarios, dispositivos y datos sensibles es enorme, estas soluciones ayudan a cerrar las brechas que los atacantes suelen aprovechar.

Desde detectar intrusiones en la red del campus hasta educar a docentes y estudiantes, estas capas extra son clave para mantener a raya las amenazas.

Categoría	Descripción de la herramienta	Qué cubre	Ejemplos
IDS/IPS	Monitoriza el tráfico de red escolar (Wi-Fi y LAN), aplica firmas + heurística y, si es IPS, bloquea ataques antes de que lleguen a los equipos.	Vulnerabilidades no parcheadas (+20% YoY) siguen circulando; especialmente en laboratorios y bibliotecas.	Snort, Suricata, Cisco Secure IPS
Análisis de vulnerabilidades	Escanea servidores de plataformas educativas, apps y contenedores; correlaciona CVEs, puntúa riesgos y sugiere parches.	34% más exploits que el año pasado; detecta puntos débiles en redes de colegios y universidades.	Nessus Expert, Qualys VMDR, Rapid7 InsightVM
Concientización & phishing sim	Plataforma e-learning con módulos micro-learning, simulaciones de phishing y métricas de mejora, ideal para staff y estudiantes.	El usuario sigue siendo el eslabón débil (60% de incidentes). Entrena, prueba, repite..	KnowBe4, Whalemate, Hook Security, Phished
Automatización de compliance	Conecta logs de sistemas escolares, mapea controles (ISO 27001, NIST, Ley 21.663) y produce reportes en un clic para directivos o ANCI.	ANCI no espera excusas: centraliza evidencias y genera reportes listos para auditoría educativa.	Vanta, Hackmetrix, Drata, Tugboat Logic

Escenario educativo realista para no morir en el intento

1. **Define tu matriz de riesgo** y prioriza herramientas donde el impacto regulatorio sea mayor (p. ej. plataformas de notas, datos de menores).
2. **Integra telemetría** (MDM → SIEM → SOAR) para correlacionar eventos y automatizar respuestas en redes escolares.
3. **Prueba tu plan B**: restaura un backup del servidor de matrícula, simula un ataque de phishing al correo institucional, dispara un playbook de contención en la red Wi-Fi del campus. La teoría sirve; la práctica salva tu lunes.dispara un playbook de contención. la teoría sirve; la práctica salva tu lunes.

> Pro-tip: ddocumenta todo el flujo. ANCI pedirá evidencias y tus futuros tú (o el próximo jefe de TI) te lo agradecerán.

07

Buenas prácticas educativas en ciberseguridad

Buenas prácticas educativas en ciberseguridad

La tecnología es una aliada clave en colegios, liceos y universidades, pero también puede convertirse en un punto débil si no se establecen prácticas sólidas de seguridad. Estas no solo ayudan a cumplir con la Ley 21.663, sino que crean una cultura de prevención que protege datos sensibles de estudiantes, docentes y administrativos.

Aplicar el principio de mínimo privilegio y Zero Trust

En entornos educativos, no todos necesitan acceso a todo. Aplica el principio de mínimo privilegio para que cada usuario (docente, estudiante, administrativo) acceda solo a la información y sistemas necesarios para su función.

Complementa esto con un enfoque **Zero Trust** que verifique continuamente identidades y dispositivos, incluso dentro de la red escolar, minimizando el riesgo de movimientos laterales de un atacante.

Rotar contraseñas institucionales

Muchas instituciones educativas mantienen contraseñas sin cambiar durante años, especialmente en redes Wi-Fi o cuentas administrativas. Esto aumenta las posibilidades de que se filtren o sean explotadas.

Establece políticas de rotación periódica y combina con autenticación multifactor (MFA) para proteger plataformas críticas como sistemas de matrícula, correos institucionales y LMS (Learning Management Systems).

Establecer reglas claras de uso para dispositivos compartidos

En colegios y universidades es común que notebooks, tablets o incluso laboratorios de computación sean utilizados por múltiples usuarios. Define normas claras: no almacenar datos personales localmente, cerrar sesión al terminar, y evitar la instalación de software no autorizado. Complementa con soluciones MDM para aplicar políticas de uso y borrar datos de forma remota si es necesario.

Comunicar cómo reportar incidentes o pérdidas de equipos

Como hemos dicho antes, reportar incidentes es una obligación bajo la Ley 21.663. Para cumplirla, debes asegurarte de que toda la comunidad educativa sepa cómo y a quién informar si detecta algo sospechoso o pierde un dispositivo. Crea canales de comunicación claros (correo dedicado, número interno, formulario online) y capacita a estudiantes y staff sobre su uso.

Simulacros frecuentes de incidentes

No basta con tener planes escritos; hay que probarlos. Organiza simulacros de incidentes como ataques de phishing dirigidos a docentes, denegaciones de servicio que afecten plataformas de clases online o pérdidas de laptops con datos de alumnos. Estas prácticas permiten evaluar la respuesta del personal, ajustar protocolos y reducir el tiempo de reacción en una crisis real.

El rol del delegado de ciberseguridad escolar

El delegado de ciberseguridad es la figura clave para mantener alineada a la institución con la Ley 21.663. Actúa como nexo directo con la ANCI, gestionando reportes y coordinando acciones de seguridad. Idealmente, debe conocer bien la infraestructura digital del colegio o universidad. Puede ser parte del área TI o contratado como apoyo externo. En centros educativos pequeños no es necesario que sea un puesto exclusivo, pero sí debe contar con respaldo institucional y tiempo asignado para cumplir sus funciones.

Responsabilidades del delegado:

¿Cuándo una institución educativa podría ser considerada OSE o estar sujeta a la ley?

- Mantener la comunicación directa con la ANCI y coordinar notificaciones de incidentes.

Si la institución es OIV:

- Supervisar la implementación y mantenimiento del SGSI (Sistema de Gestión de Seguridad de la Información).
- Liderar la gestión de incidentes: detección, contención, mitigación y reporte.
- Promover campañas de concientización en ciberseguridad para docentes, alumnos y administrativos.
- Coordinar auditorías internas y externas relacionadas con la seguridad de la información.
- Asegurar la documentación y evidencias requeridas para demostrar cumplimiento ante fiscalizaciones.
- Actualizar y revisar periódicamente los planes de continuidad operativa y recuperación ante desastres.

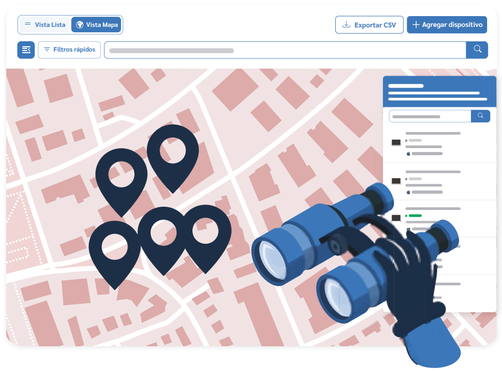
06

Cómo Prey puede ayudarte a cumplir con la Ley 21.663

Cómo Prey puede ayudarte a cumplir con la Ley 21.663

Prey ofrece una solución práctica para colegios, liceos, universidades y centros de formación que buscan cumplir con los requisitos de la Ley 21.663 sin complicaciones. Su plataforma permite gestionar, proteger y monitorear dispositivos de forma centralizada, fortaleciendo el control sobre activos críticos (como notebooks de préstamo o tablets para clases), acelerando la reacción ante incidentes y generando evidencia para auditorías, todo desde una interfaz simple y accesible.

Visibilidad y control de tu flota



En entornos educativos donde decenas o cientos de dispositivos pasan por manos de estudiantes y docentes, Prey te da una vista completa de toda la flota desde un panel centralizado. Puedes geolocalizar equipos, aplicar etiquetas (por sede, sala o departamento), y gestionar múltiples sistemas operativos (Windows, macOS, ChromeOS, Android, Ubuntu) en un solo lugar, simplificando la administración incluso en instituciones con varias sedes o campus.

Gestión de préstamos y cadena de custodia

En colegios y universidades, los notebooks y tablets vuelan de mano en mano: se asignan a cursos completos, docentes sustitutos o investigadores visitantes. Sin control central, esos equipos se evaporan fácilmente, los Excel se desactualizan y las auditorías se vuelven un dolor de cabeza. Prey simplifica todo el proceso para que cada dispositivo tenga un usuario designado, fecha de retorno clara y medidas inmediatas de protección ante incumplimientos, todo desde una sola consola, fortaleciendo así la cadena de custodia requerida por la normativa.

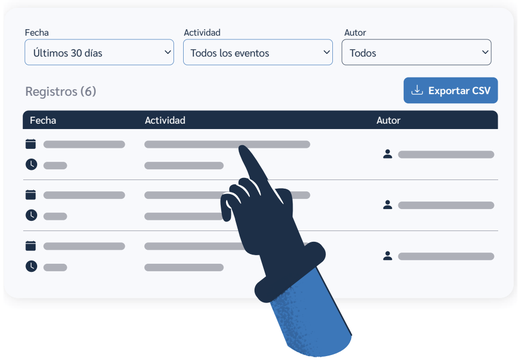
Detección de incidentes y reacción rápida

Con funciones como geofencing, alertas automáticas y detección de comportamientos inusuales (por ejemplo, acceso a la red desde ubicaciones no autorizadas), Prey permite identificar posibles incidentes en tiempo real. Además, puedes ejecutar acciones remotas como bloquear pantallas, activar alarmas o enviar mensajes a dispositivos escolares extraviados, agilizando la respuesta y minimizando el impacto en clases o exámenes online.

Protección de datos en caso de pérdida o robo

En colegios y universidades, donde los equipos suelen contener datos sensibles de alumnos, docentes y administrativos, Prey protege la información con herramientas como Remote Wipe, KillSwitch, Factory Reset y cifrado remoto con BitLocker en Windows. Esto permite borrar datos confidenciales o inutilizar equipos robados, evitando accesos no autorizados y cumpliendo con las obligaciones de salvaguarda de datos exigidas por la ley.

Evidencia y trazabilidad para auditorías



Prey mantiene un registro detallado de todas las acciones y eventos gracias a su Audit Log. Desde bloqueos remotos hasta cambios de configuración o movimientos de dispositivos, esta trazabilidad es esencial para auditorías de la ANCI y para demostrar cumplimiento en instituciones educativas que gestionan datos personales de menores.

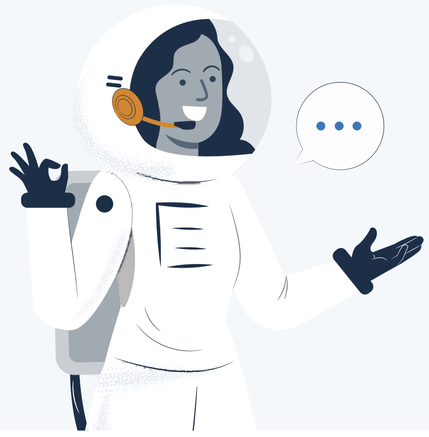
Monitoreo de brechas y credenciales en la Dark Web

Las instituciones educativas manejan diariamente miles de credenciales y datos personales que pueden filtrarse y terminar en la dark web, exponiendo plataformas académicas y administrativas a accesos no autorizados. Prey monitorea proactivamente estas filtraciones para alertar a tu equipo de TI, permitiéndote reaccionar rápidamente cambiando contraseñas o bloqueando cuentas comprometidas, mitigando riesgos y facilitando el cumplimiento de la obligación legal de informar incidentes críticos a la ANCI.

Apoyo para instituciones con bajo presupuesto

Si tu colegio o universidad aún no cuenta con los recursos necesarios para desplegar un SGSI completo basado en estándares como ISO 27001 o NIST, Prey es una alternativa efectiva, accesible y fácil de usar. Desde una sola plataforma, cubre controles esenciales como inventario actualizado, monitoreo de dispositivos, protección inmediata ante incidentes y trazabilidad completa para auditorías. Además, ofrecemos planes adaptados a la realidad y presupuesto específico de cada institución educativa, facilitando el cumplimiento sin comprometer las finanzas.

¿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

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**