Guía de cumplimiento con la

ley 21.663

en el sector salud

Prey Inc.

Por qué el sector salud es prioridad crítica en ciberseguridad

Cuando hablamos de ciberseguridad en el sector salud, no estamos hablando solo de proteger datos, sino de proteger vidas. Las instituciones médicas manejan información sumamente delicada: desde fichas clínicas y resultados de exámenes hasta diagnósticos, tratamientos en curso y datos de aseguradoras. Basta con que un sistema se caiga o se vea comprometido para que toda la operación se vea afectada: pacientes sin atención, médicos sin acceso a historiales, laboratorios detenidos.

Un caso reciente lo dejó claro: el ciberataque al Instituto de Salud Pública (ISP) en junio de 2025 paralizó procesos esenciales, afectando no solo al propio instituto, sino también a Aduanas y otros servicios sanitarios a nivel nacional. Por eso, la Ley 21.663 identifica expresamente al sector salud como un servicio esencial, lo que implica que muchas clínicas, hospitales y laboratorios deben cumplir obligaciones de ciberseguridad mucho más estrictas.

Esta guía nace para ayudarte a entender ese nuevo marco legal y dar pasos concretos para proteger tu institución, tu operación y más importante, tus pacientes.

01

¿Mi organización está obligada a cumplir?

¿Mi organización está obligada a cumplir?

Si trabajas en una clínica, hospital, consultorio, centro médico o en el ámbito de la investigación y producción de productos farmacéuticos, la respuesta corta es: sí, probablemente estás obligado a cumplir con la Ley 21.663. Según el artículo 4° de esta ley, los servicios de atención en salud —ya sean públicos o privados— están expresamente definidos como servicios esenciales. Esto significa que cualquier institución que preste servicios médicos, desde grandes hospitales hasta centros ambulatorios, queda dentro del alcance de la normativa.

Y eso no es todo. Si tu operación depende del uso de redes, sistemas informáticos o software clínico para funcionar —lo cual es prácticamente inevitable hoy en día— y además una interrupción de tus servicios podría afectar la atención médica, la seguridad pública o la capacidad del Estado para garantizar servicios de salud, puedes ser designado como Operador de Servicios Esenciales (OSE) o como Operador de Importancia Vital (OIV). Esto está regulado en el artículo 5° de la misma ley. Es decir, si manejas datos sensibles, atiendes urgencias, prestas servicios a gran escala o formas parte de una red de atención, estás directamente bajo el radar de la Agencia Nacional de Ciberseguridad (ANCI).

¿Y si aún no estás designado? Igual deberías prepararte.

Hoy en día, es prácticamente imposible que una institución de salud funcione sin plataformas digitales. Si tu clínica o centro médico depende de software de gestión clínica, fichas electrónicas, portales web o acceso remoto a información médica, ya estás expuesto a riesgos que esta ley busca controlar. Lo mismo si usas tablets, laptops, celulares u otros dispositivos para acceder a información de pacientes. Además, si formas parte de una red pública o privada de atención médica, tus obligaciones pueden extenderse más allá de tu organización individual: el cumplimiento se vuelve parte del ecosistema.

En este escenario, anticiparse es clave. La ANCI puede designar nuevas entidades en cualquier momento si cumplen con los criterios legales. No esperes una notificación formal para empezar a proteger a tus pacientes, tus sistemas y tu reputación. Implementar medidas preventivas ahora puede marcar la diferencia más adelante.

Autoevaluación rápida: ¿Estás en la mira?

Pregunta	"sí" significa...
¿Prestas servicios médicos como hospital, clínica, consultorio o centro médico?	Estás explícitamente en la categoría de servicio esencial (Art. 4°).
¿Tu institución depende de sistemas informáticos o software clínico para funcionar?	Cumples con el primer requisito de OIV (Art. 5°).
¿Una interrupción de tus servicios podría afectar la atención médica o la seguridad pública?	Cumples con el segundo requisito de OIV (Art. 5°).
¿Tienes dispositivos (laptops, tablets, celulares) con acceso a información de pacientes?	Punto crítico de exposición digital.
¿Formas parte de una red de atención pública o privada?	Mayor probabilidad de ser fiscalizado o designado.
¿Recibiste algún oficio o consulta de la ANCI o el CSIRT de salud?	Estás en proceso de evaluación. Empieza con tu SGSI hoy.

¿Qué hacer según tus respuestas?

- **3 o más "SÍ":** Actúa como si ya fueras OSE/OIV. Las obligaciones legales ya están en vigor.
- **1-2 "SÍ":** Implementa controles clave y prepárate para una eventual designación.
- **0 "SÍ":** Aun así, el riesgo sigue ahí. La prevención también es parte del cuidado del paciente.

02 Riesgos digitales específicos en salud

Riesgos digitales específicos en salud

Cuando hablamos de ciberseguridad en el sector salud, no lo hacemos por exagerar: lo hacemos con datos. Según el último Data Breach Investigations Report (DBIR) de Verizon, el sector sanitario sigue siendo uno de los más atacados, y no solo por lo valiosa que es su información, sino también por lo crítica que es su operación. Vamos a repasar los principales riesgos, con cifras que te van a dejar pensando.

Robo o extravío de dispositivos con fichas médicas

Los dispositivos móviles —como laptops, tablets o celulares— son parte del día a día en clínicas y hospitales. Pero también representan un riesgo muy real. El DBIR muestra que el uso indebido de activos físicos, como el robo o pérdida de dispositivos, sigue siendo una causa significativa de incidentes en el sector salud. Si esos equipos contienen información no cifrada o accesos sin protección, una simple pérdida puede transformarse en una brecha grave de datos personales.

Ataques de ransomware que bloquean el acceso a historiales clínicos

El ransomware no afloja. Según el DBIR, este tipo de ataque representa el 44% de las brechas de seguridad. ¿El problema? No se trata solo de pagar un rescate. Cuando los historiales clínicos quedan bloqueados, se detiene la atención médica, se interrumpen tratamientos y se pone en riesgo la seguridad de los pacientes. Y lo más preocupante: muchas veces estos ataques no llegan solos, vienen acompañados de robo de datos o amenazas de filtración.

Phishing a personal administrativo o médico

El phishing sigue siendo la puerta de entrada favorita de los atacantes. El informe de Verizon indica que el robo de credenciales está presente en el 22 % de las brechas y que el phishing representa el 16% de los vectores iniciales. En el entorno clínico, basta con que alguien haga clic en un correo malicioso para que todo el sistema quede expuesto. Y como muchos usuarios tienen acceso simultáneo a fichas, recetas y sistemas financieros, el daño puede ser enorme.

Interrupción de servicios críticos (ambulancias, urgencias, laboratorio)

Más allá de los datos, está la operación clínica. El informe de Verizon subraya que muchas brechas en salud tienen un impacto operativo inmediato, y no es sorpresa que los atacantes tengan pocas morales como para no importarles las consecuencias de paralizar un hospital. Si un sistema de ambulancias cae por un ataque, no es solo un problema TI: es una emergencia nacional.

Accesos indebidos a sistemas de prescripción, pagos o exámenes Los errores humanos siguen siendo parte importante del problema. El DBIR destaca que el 74% de los incidentes en salud se deben a una mezcla de intrusión de sistemas y fallas internas, como accesos indebidos, configuraciones erróneas o exposición accidental de información. Un clic equivocado o una mala configuración en un sistema de prescripción puede no solo vulnerar datos, sino afectar directamente la atención al paciente.

03 Obligaciones principales según la ley (versión salud)

Obligaciones principales según la ley (versión salud)

Si trabajas en una clínica, hospital, laboratorio o centro médico —ya sea público o privado— es momento de prestar atención. La Ley 21.663 no es solo otra norma técnica: define obligaciones concretas para que los servicios esenciales de salud puedan anticiparse, actuar rápido y recuperarse ante incidentes cibernéticos graves que puedan afectar la atención de pacientes o poner en riesgo su información clínica.

¿Ya trabajas con ISO 27001, algún SGSI o protocolos del Ministerio de Salud? Buen comienzo. Pero esta ley exige más que políticas en papel: se trata de demostrar, con hechos y evidencia, que tu institución está preparada para enfrentar un ciberataque. Aquí te mostramos las principales obligaciones que debes conocer si estás en el sector salud:

Registro obligatorio en el portal de la ANCI

OSE : ✓ **OIV:** ✓

Este es el primer paso formal. Toda institución clasificada como **Prestador de Servicios Esenciales (OSE)** o **Operador de Importancia Vital (OIV)** debe registrarse en el portal oficial de la ANCI. Si tu hospital, clínica o centro médico presta atención continua o participa en redes asistenciales, ya entras en esta categoría.

El registro permite que la ANCI te supervise, te entregue lineamientos específicos y coordine respuestas en caso de incidentes.

El portal ANCI ya está activo desde el 11 de junio de 2025: **portal ANCI:**

Designación de un delegado de ciberseguridad

OSE : ✓ **OIV:** ✓

La ley exige que las instituciones catalogadas como OSE u OIV cuenten con un delegado formal, designado por la alta dirección. Este será el punto de contacto con la ANCI y debe tener experiencia o formación en el área. Este responsable no solo coordina las acciones internas de seguridad, sino que también se encarga de informar a la alta dirección sobre riesgos y cumplimiento, además de liderar la respuesta ante incidentes.

SGSI activo y documentado

OSE : ✗ | OIV: ✓

Los OIV deben tener un Sistema de Gestión de Seguridad de la Información (SGSI) en funcionamiento real, no solo en papel. Esto significa que tu institución debe tener políticas activas, controles aplicados y evidencia clara de que todo esto se está cumpliendo.

En salud, esto incluye proteger historiales clínicos, controlar el acceso a sistemas médicos, realizar evaluaciones de riesgo y capacitar al personal. Si ya sigues ISO 27001, vas bien encaminado, pero tendrás que alinearlo con los requerimientos específicos de la ley.

[Guía práctica sobre SGSI e ISO 27001 en entornos clínicos]

Reporte de incidentes: en menos de 3 horas

OSE : ✓ | OIV: ✓

Cuando ocurre un incidente cibernético, el tiempo cuenta. Todas las instituciones clasificadas como OSE u OIV deben notificar al CSIRT Nacional dentro de las 3 horas siguientes a su detección.

El proceso tiene tres etapas:

1. **Alerta inicial en máximo 3 horas.**
2. **Informe preliminar en 72 horas (24h si eres OIV).**
3. **Informe final en 15 días corridos.**

Esto es especialmente relevante si un ciberataque afecta urgencias, sistemas de turnos o plataformas de atención a pacientes.

[Consulta los formatos oficiales en el Decreto N° 295 y Resolución N° 7/2025]

Auditorías, análisis de riesgos y simulacros

OSE : ✗ | OIV: ✓

Las instituciones de salud clasificadas como OIV deben realizar auditorías periódicas, internas y externas, así como simulacros de ciberincidentes.

Ejemplos:

- **Simular una pérdida de fichas médicas.**
- **Evaluar qué pasa si se cae el sistema de urgencias.**
- **Ver si los backups realmente funcionan.**

Todo debe quedar documentado para demostrar que tu equipo sabe qué hacer.

Planes de continuidad operacional y ciberseguridad

OSE : ✗ | OIV: ✓

¿Puedes seguir atendiendo pacientes si tu sistema clínico cae? ¿Qué haces si pierdes conexión con laboratorios o ambulancias?

La ley exige que los OIV cuenten con **planes actualizados de continuidad operativa y ciberseguridad**, validados al menos cada dos años. Estos planes deben permitirte seguir funcionando ante cualquier incidente crítico.

[Crea tu plan de respuesta a incidentes de ciberseguridad]

Medidas inmediatas para contener incidentes

OSE : ✗ | OIV: ✓

No basta con detectar un ataque: hay que saber actuar. Las instituciones OIV deben tener capacidad de contención inmediata. En salud, esto puede incluir:

- **Bloquear accesos comprometidos.**
- **Aislar equipos infectados.**
- **Restaurar sistemas desde copias seguras.**

Certificaciones de respaldo

OSE : ✗ | OIV: ✓

La ANCI puede exigir que los OIV presenten certificaciones como ISO 27001 para validar la madurez de su SGSI. Aunque los OSE no están obligados, tener estas certificaciones es una ventaja al momento de demostrar cumplimiento y reducir sanciones ante una auditoría.

Notificación a potenciales afectados

OSE : ✗ | OIV: ✓

Si el incidente pone en riesgo los datos de pacientes u otros servicios críticos, y la ANCI lo instruye, tu institución deberá notificar a los afectados. Esto incluye informar sobre el tipo de datos expuestos y qué medidas se tomarán para protegerlos.

Programas de capacitación y campañas de ciberhigiene

OSE : ✗ | OIV: ✓

El personal clínico y administrativo debe ser parte activa de la defensa digital. La ley exige programas de formación continua para prevenir errores humanos, como caídas en phishing, mal uso de contraseñas o pérdida de dispositivos. En entornos donde cada segundo cuenta, saber cómo actuar marca la diferencia.

Cumplimiento de normativas técnicas ANCI o sectoriales

OSE : ✓ | OIV: ✓

Finalmente, todas las instituciones deben alinearse con las normativas técnicas que dicte la ANCI. En el caso del sector salud, también puede haber lineamientos del Ministerio de Salud o de redes asistenciales regionales. La clave está en integrar lo que ya existe con los nuevos requerimientos de trazabilidad, reporte y respuesta exigidos por la ley.

Checklist descargable para cumplir con la Ley 21.663

04

Qué pasa si no cumples

Qué pasa si no cumples

En ciberseguridad, el “no sabía” no te libra de las consecuencias. La Ley 21.663 establece un sistema de sanciones que clasifica las infracciones en tres niveles: leves, graves y gravísimas, dependiendo del impacto y la gravedad del incumplimiento. Y en el caso del sector salud, donde una interrupción puede afectar tratamientos, urgencias o el acceso a medicamentos, las sanciones pueden escalar rápido.

Por ejemplo, no reportar un ciberataque que dejó fuera de línea tu sistema de urgencias, o no avisar a pacientes cuyos datos fueron filtrados, puede convertirse en una infracción gravísima, con multas de hasta 40.000 UTM si eres OIV. Además, dependiendo de la situación, la ANCI puede imponer sanciones adicionales como inhabilitaciones operativas o requerir auditorías externas inmediatas.

Tipo de infracción	Definición breve	Multa máxima (OSE)	Multa máxima (OIV)
Leve	Incumplimientos menores o administrativos sin impacto directo.	5.000 UTM	10.000 UTM
Grave	No aplicar estándares, omitir reportes críticos, entorpecer fiscalizaciones.	10.000 UTM	20.000 UTM
Gravísima	Reincidencia grave o incidentes con alto impacto sobre servicios esenciales.	20.000 UTM	40.000 UTM

Tipos de infracciones según el artículo 38

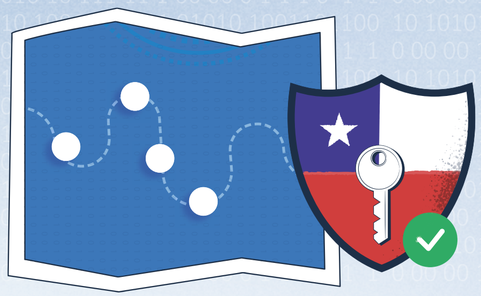
Categoría Infracciones	Infracciones OSE	Infracciones OIV
Infracciones Leves	• Entregar tarde información solicitada por la ANCI sobre medidas de seguridad. - No seguir una instrucción menor de la ANCI (ej. actualizar protocolo interno).	• No designar un delegado de ciberseguridad. • No documentar acciones de seguridad. • No realizar capacitaciones al personal médico/ administrativo. • No tener planes de continuidad certificados.
Infracciones Graves	• No reportar un incidente que afectó el sistema de turnos. • No seguir los protocolos sectoriales emitidos por la ANCI o MINSAL.	• No implementar un SGSI. • No activar el plan de continuidad tras un ataque. • No informar a los pacientes afectados por una filtración de datos médicos. • Reincidir en una infracción leve en menos de un año.
Infracciones Gravísimas	• Entregar información falsa durante un incidente crítico. • Negarse a colaborar con la ANCI ante un ciberataque a servicios de urgencia.	• No tomar medidas de contención cuando hay un ransomware activo. • Reincidir en una infracción grave que afecte la atención clínica.

¿Qué factores pueden agravar la sanción?

Las sanciones pueden aumentar considerablemente si se presentan ciertos factores agravantes. La reincidencia es uno de los más comunes: cometer la misma infracción más de una vez en un año eleva la gravedad automáticamente. También influye el impacto social o clínico del incidente. Además, el tamaño y la criticidad de la institución también pesan.

Imagina que una clínica privada es víctima de un ataque que expone cientos de fichas clínicas. No informa al CSIRT en el plazo legal (3 horas), ni a los pacientes. Tampoco documenta medidas de contención. Resultado: infracción grave que puede escalar a gravísima si se comprueba negligencia, con multas de hasta 40.000 UTM y revisión completa de sus sistemas.

05



Pasos prácticos para cumplir

Pasos prácticos para cumplir

Cumplir con la Ley 21.663 no significa transformar tu clínica en un centro tecnológico de un día para otro. Pero sí requiere orden, claridad y decisiones clave. Lo importante es partir por lo esencial y avanzar con pasos concretos. Aquí te dejamos un plan simple para empezar, pensado especialmente para instituciones del área de la salud.

Diagnóstico inicial

Antes de tomar decisiones, necesitas entender tu realidad. Un buen diagnóstico te permite saber por dónde partir y qué tan expuesta está tu institución. Hoy en día, casi todos los centros de salud trabajan con fichas electrónicas, sistemas de laboratorio o plataformas de agendamiento. Y la mayoría accede a ellas desde múltiples dispositivos.

Pasos del diagnóstico inicial:

1. **Inventario de activos:** Haz un inventario completo de todos los activos de información: dispositivos físicos como laptops y servidores, sistemas operativos, redes, aplicaciones y datos sensibles. Este paso es clave para saber qué necesitas proteger y para identificar qué tan expuesto está tu entorno actual a posibles amenazas.
2. **Análisis de riesgos:** Realiza un análisis detallado de las amenazas que podrían afectar tu operación, considerando vulnerabilidades internas y externas. Evalúa la probabilidad de que ocurran incidentes y el impacto que tendrían sobre tus servicios esenciales, usuarios y reputación. Esta información te ayudará a priorizar las acciones de seguridad más críticas.
3. **Revisión de políticas actuales:** Examina si ya existen políticas o procedimientos relacionados con la seguridad de la información. Pregúntate: ¿cubren realmente los riesgos actuales? ¿Están alineadas con estándares como ISO 27001? Este análisis permite identificar vacíos normativos y ajustar la gobernanza antes de implementar un SGSI.
4. **Mapeo de procesos:** Identifica cómo se mueve la información dentro de la organización: quién accede a qué datos, cómo se comparten y dónde podrían existir puntos débiles. El objetivo es visualizar el flujo de trabajo y encontrar procesos que requieran controles adicionales para proteger 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 las áreas críticas según su riesgo e impacto potencial. Este documento servirá como base para tu plan de acción y te permitirá demostrar a la dirección la necesidad de invertir en seguridad.

Recursos adicionales para el sector TI:

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

Designa un responsable de ciberseguridad

No necesitas tener un equipo TI completo, pero alguien tiene que asumir el rol de liderar este tema. Puede ser alguien interno con formación en el área, o un proveedor externo que actúe como delegado de ciberseguridad. Lo importante es que tenga claridad sobre tus sistemas clínicos, pueda coordinar acciones en caso de incidentes y sea el punto de contacto con la ANCI si llegas a ser clasificado como OSE u OIV.

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

Elegir un marco sólido es como definir el blueprint de tu ciberseguridad. Si eres una institución de salud grande 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 de ciberseguridad, 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	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

Una gran parte de los incidentes se originan por errores humanos. Por eso, capacitar al personal no técnico es clave. No necesitas volver expertos en ciberseguridad a médicos o administrativos, pero sí enseñarles prácticas básicas: reconocer correos falsos, no compartir contraseñas, bloquear el equipo al ausentarse. Pequeños cambios que previenen grandes problemas.

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

¿Qué pasa si un ataque de ransomware bloquea el acceso a fichas clínicas o deja inoperativo el sistema de urgencias? Ahí es donde entra el Plan de Continuidad Operativa (PCO): un esquema claro para seguir funcionando, incluso en medio del caos. Este plan debe definirse, probarse regularmente y mantenerse actualizado, en especial si tu organización cuenta como OIV ya que es obligatorio tener uno.

Para armarlo bien, puedes guiarte por la norma ISO 22301, que establece buenas prácticas para la continuidad del negocio. Tener un PCO sólido no solo es clave ante ciberataques, también sirve frente a cortes de energía, fallos técnicos o cualquier evento que afecte tus operaciones clínicas.

¿Qué debe incluir un PCO y un plan de respuesta en instituciones de salud?

- **Identificación de procesos clínicos críticos:** Sistemas que no pueden fallar, como el acceso a la ficha clínica electrónica, el sistema de urgencias, RIS/PACS, y plataformas de laboratorio.
- **Evaluación de riesgos y análisis de impacto operativo:** Desde pérdida de conectividad con el Ministerio de Salud hasta corrupción de bases de datos de pacientes o indisponibilidad de recetas electrónicas.
- **Protocolos de respuesta inmediata:** Aislamiento de equipos comprometidos, activación de planes de contingencia manuales, y reporte de incidentes al CSIRT Nacional en menos de 3 horas.
- **Roles y responsabilidades claras:** El CISO o encargado de seguridad, TI hospitalaria, jefes de servicio clínico, y personal administrativo deben saber qué hacer y cuándo actuar.
- **Simulacros y entrenamientos periódicos:** Validar la reacción de los equipos ante incidentes reales o simulados, midiendo tiempos de respuesta y capacidad de recuperación.
- **Planes de recuperación tecnológica y clínica:** Restaurar servicios digitales (HIS, LIS, ERP), accesos remotos y bases de datos sin afectar la continuidad de atención.
- **Lecciones aprendidas y mejora continua:** Tras cada incidente o simulacro, documentar errores, aciertos y ajustar procedimientos para fortalecer la resiliencia operativa.

Pruebas, simulacros y auditorías

Tener un plan en papel es un buen comienzo, pero ¿funciona en condiciones reales? En el ámbito de la salud, donde cada segundo puede marcar la diferencia entre la vida y la muerte, probar tus planes de continuidad y seguridad no es opcional. La única forma de garantizar que responderás de manera efectiva ante un incidente es mediante pruebas técnicas, simulacros clínico-digitales y auditorías periódicas.

Además, la Ley 21.663 exige a los OSE y OIV del sector salud realizar revisiones al menos cada dos años para conservar su estado de cumplimiento y su operatividad certificada.

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.	Restauración de backups del HIS, failover de servidores clínicos, validación de alertas automáticas en sistemas de monitoreo.
Simulacros	Ejercicios prácticos donde los equipos simulan responder a ataques.	Entrena al personal y mide la coordinación bajo presión.	Ataques simulados a la red hospitalaria, pérdida de acceso a ficha clínica, caída de RIS/PACS; cronómetro en mano.
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/externas, entrevistas a encargados TI y clínicos, revisión de incidentes reales.

Documentación y evidencia

En ciberseguridad hospitalaria, lo que no está documentado no existe para los auditores... ni para la ANCI. La Ley 21.663 exige mantener registros detallados y actualizados que demuestren la aplicación real de las medidas de seguridad, algo fundamental para reconstruir incidentes (¿quién accedió a la ficha del paciente? ¿qué servicios estaban operativos?) y proteger la confianza de tus pacientes y organismos reguladores.

Documentación crítica que deberías tener lista:

- **Políticas y procedimientos:**
  - Política de seguridad de la información (alineada al área clínica y actualizada).
  - Procedimiento ante incidentes TI que afecten la atención médica.
  - Planes de continuidad operativa y recuperación ante fallas tecnológicas.
- **Registros de actividad y trazabilidad:**
  - Logs de acceso a fichas clínicas, RIS, LIS y servidores críticos.
  - Cambios en infraestructura de red hospitalaria (on-prem o cloud).
  - Acciones ejecutadas con herramientas como **Prey** (borrado remoto de portátiles, bloqueos, localización de tablets de atención domiciliaria).
- **Evidencia de formación del personal:**
  - Registros de capacitaciones a equipos clínicos, administrativos y de TI.
  - Resultados de campañas de concientización sobre phishing o uso seguro de sistemas.
  - Certificados y métricas de participación.
- **Informes de simulacros y auditorías:**
  - Resultados de pruebas periódicas sobre ciberataques simulados.
  - Hallazgos, acciones correctivas y lecciones aprendidas tras ejercicios reales.
  - Evidencia de cumplimiento entregada a la ANCI o CSIRT de Salud.
- **Certificaciones y cumplimiento**
  - Certificaciones ISO 27001 / 22301 (si ya aplican).
  - Documentación de revisiones bianuales y cumplimiento de medidas exigidas.
- **Inventario de equipos médicos y TI:**
  - Laptops, tablets y terminales clínicas, con sus responsables designados.
  - Equipos médicos conectados (IoMT), como monitores, bombas de infusión, sensores.
  - Infraestructura de red (routers, firewalls) y unidades de respaldo.
  - Dispositivos móviles de atención en terreno o telemedicina.

Implementación de políticas y controles

Aquí es donde se pasa del documento a la acción. Un SGSI hospitalario efectivo exige políticas claras sobre quién accede a qué información, con controles técnicos que respalden esas decisiones.

Ejemplos clave en entornos clínico-tecnológicos:

- **Control de accesos según rol (RBAC):** Un médico no necesita acceso a infraestructura TI, y el equipo de soporte técnico no debe tener permisos para modificar fichas clínicas.
- **Contraseñas y MFA:** Autenticación robusta para accesos a sistemas hospitalarios, VPNs y portales de prescripción electrónica.
- **Parches y actualizaciones automáticas:** En sistemas de gestión clínica, RIS/PACS, y terminales móviles de atención.
- **Cifrado de datos clínicos:** Protege registros médicos en tránsito y en reposo.
- **Segmentación de redes hospitalarias:** Separa áreas críticas como laboratorio, urgencias y administración para contener un posible incidente. Este control es especialmente vital en clínicas y hospitales que externalizan servicios a MSPs o proveedores de sistemas SaaS de salud. Un error de configuración puede comprometer toda la operación clínica.

Gestión de flota de dispositivos con herramientas simples

Con profesionales de salud trabajando desde centros asistenciales, terreno o en formato híbrido, necesitas visibilidad total de tu flota digital. El inventario en papel ya no basta. Una solución MDM/UEM te permite aplicar políticas de seguridad, rastrear equipos extraviados y cumplir con los requerimientos de auditoría.

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 personal clínico, configurar alertas automáticas (geofencing, batería baja, cambios de hardware) y mantener un historial de acciones ejecutadas para auditorías.

Herramientas tecnológicas recomendadas

En ciberseguridad clínica, confiar solo en un antivirus es como pensar que basta con un solo antibiótico para curar todos los males. Hoy, gran parte de la atención médica depende de sistemas digitales: desde fichas electrónicas y recetas, hasta exámenes, pagos y agendas. Si quieres proteger la salud de tus pacientes y la reputación de tu centro médico, necesitas un stack de seguridad serio y alineado con los riesgos reales del sector.

A continuación, te mostramos las herramientas clave que toda institución de salud debería considerar. Además, incluimos datos del Data Breach Investigations Report 2025 de Verizon, para entender por qué estos controles son más urgentes que nunca.

Categoría	Descripción de la herramienta	Por qué importa	Ejemplos
MDM (monitoreo de dispositivos)	Monitorea tablets, laptops y celulares usados por personal médico y administrativo. Permite aplicar políticas, rastrear, bloquear o borrar datos de forma remota.	El **22% de las brechas** comenzaron por dispositivos sin visibilidad ni control.	Prey , Microsoft Intune, Jamf Pro
Gestión de parches	Actualiza software clínico y operativo, prioriza vulnerabilidades críticas (CVE) y verifica instalación.	El **20% de los ataques** explotó vulnerabilidades.	Automox, WSUS, Ivanti Neurons
Protección de endpoints (AV + EDR)	Detiene malware y ransomware, detecta comportamientos sospechosos en tiempo real y aísla equipos.	El **44% de las brechas** involucró ransomware.	CrowdStrike Falcon, SentinelOne, Bitdefender
SIEM / UEBA	Recoge logs de múltiples fuentes, detecta patrones inusuales (como accesos indebidos a fichas clínicas) y alerta en tiempo real.	**60% de los incidentes** involucran errores o acciones humanas.	Microsoft Sentinel, IBM QRadar, Elastic SIEM
Backups 3-2-1	Copias de seguridad locales + nube, con validación y protección contra alteraciones o ransomware.	Sin backups, no hay vuelta atrás ante un ataque.	Veeam, Acronis, MSP360
Gestor de contraseñas	Crea, guarda y comparte credenciales cifradas de forma segura.	El **22% de los incidentes** partieron con credenciales robadas.	Bitwarden, 1Password, Keeper
IAM / CABS	Administra accesos según perfil (médico, técnico, administrativo), con MFA y control granular.	Solo accede quien debe, cuando debe.	Okta, Azure AD, JumpCloud
Firewall perimetral / cloud	Segmenta redes internas (urgencias, laboratorio, recepción) y aplica reglas Zero Trust para bloquear amenazas.	**22% de las brechas** usaron accesos mal protegidos.	Palo Alto, Fortinet, Zscaler

Herramientas complementarias

Estas soluciones complementan el stack básico y son especialmente útiles en entornos clínicos donde hay múltiples usuarios, datos sensibles y una necesidad crítica de continuidad operativa.

Categoría	Descripción de la herramienta	Qué cubre	Ejemplos
IDS/IPS	Monitorea el tráfico de red clínica y bloquea intentos de ataque en tiempo real.	Detecta vulnerabilidades antes de que impacten.	Snort, Suricata, Cisco Secure IPS
Análisis de vulnerabilidades	Escanea equipos, apps y servidores para identificar riesgos antes de que sean explotados.	Prioriza fallas críticas que podrían afectar atención médica.	Nessus, Qualys, Rapid7 InsightVM
Concientización & phishing sim	Entrena al personal médico y administrativo con simulaciones reales y microcursos.	El eslabón humano sigue siendo el más débil.	KnowBe4, Hook Security, Phished
Automatización de compliance	Alinea controles con ISO 27001 y la Ley 21.663, y genera evidencias listas para auditoría.	Ahorra tiempo y evita multas.	Hackmetrix, Drata, Vanta
DLP (prevención de pérdida de datos)	Detecta y bloquea intentos de fuga de información clínica, ya sea por error o intencionalmente.	Protege fichas médicas y exámenes frente a extracciones no autorizadas.	Endpoint Protector, Forcepoint DLP, Microsoft Purview
Automatización de compliance	Asigna y restringe accesos según funciones: médicos, técnicos, administrativos.	Reduce el riesgo de accesos indebidos a información clínica.	BeyondTrust, CyberArk, Ekran System

1. **Evalúa tu exposición:** ¿tienes dispositivos sin monitoreo? ¿copias de seguridad validadas?
2. **Prioriza por riesgo:** ficha clínica, prescripciones, resultados de laboratorio y pagos deben estar siempre protegidos.
3. **Haz pruebas:** simula una pérdida de laptop, un ataque de phishing o la caída del sistema de urgencias. Verifica cómo responde tu stack de seguridad.

> Consejo final: no esperes a estar en la lista de OSE/OIV para actuar. En salud, los daños de un ciberataque se miden en minutos... y en vidas.

06 Buenas prácticas de ciberseguridad para el entorno clínico

Buenas prácticas de ciberseguridad para el entorno clínico

No todo depende de la tecnología. Muchas veces, lo que marca la diferencia es cómo se comporta el equipo humano frente a situaciones de riesgo. En un entorno clínico, donde hay múltiples turnos, personas y dispositivos circulando, aplicar buenas prácticas de ciberseguridad es tan importante como tener el mejor software.

Separar dispositivos de uso personal de los que acceden a datos médicos

Usar el mismo celular para WhatsApp personal y para revisar fichas clínicas es una receta para el desastre. Separar lo profesional de lo personal ayuda a mantener los datos médicos bajo control y evita exponer información sensible por descuido.

Beneficios de separar dispositivos:

1. Reduces el riesgo de fugas de datos por apps personales.
2. Facilitas el monitoreo y cumplimiento normativo.
3. Simplificas acciones de bloqueo o borrado remoto en caso de pérdida.
4. Evitas conflictos de privacidad entre datos personales y laborales.

Establecer protocolos para pérdida o robo de equipos con acceso a fichas

Cuando un equipo con datos clínicos se pierde o es robado, cada minuto cuenta. Tener protocolos claros permite reaccionar de inmediato: reportar, bloquear, rastrear, y si es necesario, borrar remotamente la información. Sin este plan, el caos se apodera del proceso y los datos quedan expuestos.

Capacitar al personal de recepción y atención al paciente: son la primera línea

El primer contacto en una clínica no siempre es con un médico, sino con alguien en recepción. Este personal también maneja datos sensibles, desde rut hasta información de seguros, y debe estar preparado para reconocer riesgos.

¿Qué deben aprender?

- Cómo identificar correos o llamados sospechosos (phishing, ingeniería social).
- Qué hacer si se pierde un dispositivo o hay una brecha de datos.
- Buenas prácticas al usar contraseñas y cerrar sesiones.
- Cuándo y cómo escalar un posible incidente de seguridad.

¿Cómo capacitarlos de forma efectiva?

- **Plataformas de e-learning** con módulos breves, medibles y certificados.
- **Charlas cortas mensuales** de 15–30 min con ejemplos reales.
- **Correos educativos semanales** con tips rápidos y recordatorios visuales.
- **Simulacros de phishing** para medir y mejorar su respuesta.
- **Afiches visibles** en zonas comunes con prácticas seguras.

El delegado de ciberseguridad en instituciones de salud

La Ley 21.663 exige que toda institución clasificada como OIV y, recomendable para los OSE, tenga un delegado de ciberseguridad formalmente designado con un documento firmado por el representante legal. Esta persona no solo debe conocer de seguridad informática, sino entender los riesgos específicos del entorno clínico y cómo afectan la continuidad de la atención.

Debe conocer los sistemas clínicos y tecnológicos

Aunque no tiene que ser médico, es un gran plus si el delegado entiende de regulaciones del sector, y otras cosas, como el funcionamiento de las fichas electrónicas, los sistemas de prescripción o la interoperabilidad con Fonasa y laboratorios externos. Esto le permitirá tomar decisiones más acertadas, ajustar políticas a la realidad del centro y anticiparse a posibles riesgos que no siempre se ven desde TI.

Perfil técnico o mixto, con conocimiento regulatorio

El delegado debe saber tanto de ciberseguridad como de normativas. No basta con manejar firewalls; debe comprender la Ley 21.663, la ISO 27001, PCI DSS y los requisitos de la CMF. Idealmente, combina habilidades técnicas con visión estratégica y experiencia en gestión. En el sector financiero, este mix no es un plus: es lo mínimo.

Actúa como vínculo directo con la ANCI

Este delegado será la cara visible de tu institución ante la Agencia Nacional de Ciberseguridad. Su rol es clave en auditorías, reportes y coordinaciones durante un incidente.

Responsabilidades principales del delegado:

- Coordinar el cumplimiento de la Ley 21.663 dentro del centro de salud.
- Reportar incidentes al CSIRT Nacional.
- Centralizar la documentación de seguridad y continuidad operativa.
- Participar (o liderar) auditorías, simulacros y capacitaciones.
- Ser punto de contacto en procesos de fiscalización.

Puede ser alguien del área TI o contratado externamente con ese fin

No es obligatorio que el delegado sea parte del staff interno. Puedes designar a alguien externo, como un proveedor de ciberseguridad o un consultor con experiencia. Lo importante es que esté disponible, conozca bien tus operaciones clínicas y tenga la confianza del equipo directivo. Al final del día, será quien represente tu compromiso con la seguridad digital frente al regulador.

07

Cómo Prey puede ayudarte a cumplir con la Ley 21.663 en salud

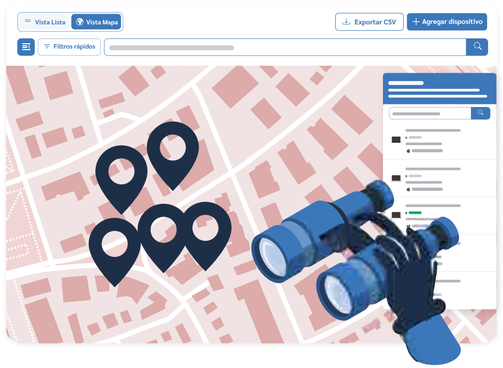
Cómo Prey puede ayudarte a cumplir con la Ley 21.663 en salud

Las instituciones de salud trabajan con información altamente sensible y equipos que no siempre están bajo llave: tablets en box de atención, notebooks en visitas domiciliarias, celulares del equipo clínico... y todos con acceso a fichas médicas. Prey te ayuda a proteger esos dispositivos, cumplir con la Ley 21.663 y ganar trazabilidad operativa sin complicar tu día a día ni tu presupuesto.

Detección y alertas automáticas ante comportamientos sospechosos

Con funcionalidades como geofencing, alertas por movimiento no autorizado y monitoreo de comportamientos anómalos, Prey te permite actuar al instante si un dispositivo sale de su perímetro o muestra señales de riesgo. Puedes bloquearlo, enviar mensajes o borrar la información remotamente antes de que ocurra un acceso indebido.

Monitorea y protege dispositivos móviles con acceso a datos clínicos

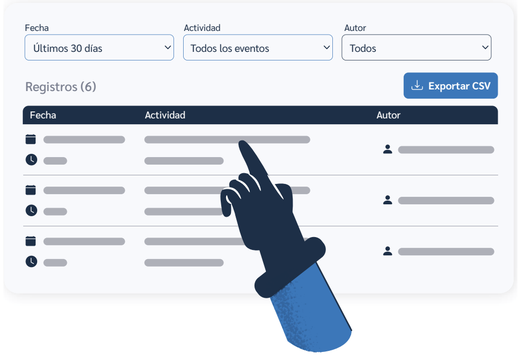


Prey te muestra en un solo panel dónde están todos tus equipos —desde los PC de recepción hasta los móviles del personal de urgencia—. Puedes etiquetar dispositivos por unidad, tipo o responsable, aplicar filtros personalizados y administrar múltiples sistemas operativos (Windows, macOS, Android, Ubuntu, ChromeOS), incluso en contextos mixtos o con dispositivos compartidos por turno.

Bloqueo remoto y borrado de información médica en caso de pérdida o robo

Una ficha médica expuesta es más que un dato filtrado: es una posible vulneración de la ley. Por eso, Prey incluye funciones como borrado remoto, restablecimiento de fábrica y cifrado vía BitLocker para dispositivos Windows. Así puedes cumplir con tu deber de protección y mitigar daños ante cualquier incidente.

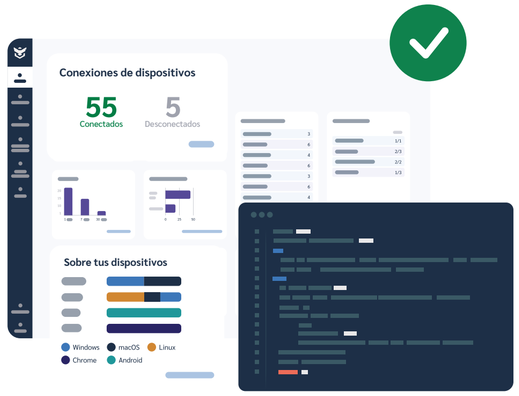
Trazabilidad y evidencia para auditorías clínicas



¿Te piden evidencias en una auditoría? Con Prey no necesitas armar todo a última hora. Su registro de actividad (Audit Log) documenta cada movimiento: desde quién accedió a qué equipo, hasta qué acciones remotas se ejecutaron y cuándo. Ideal para mostrar cumplimiento ante fiscalizaciones de la ANCI o procesos internos de calidad.

Alerta temprana con Dark Web Monitoring

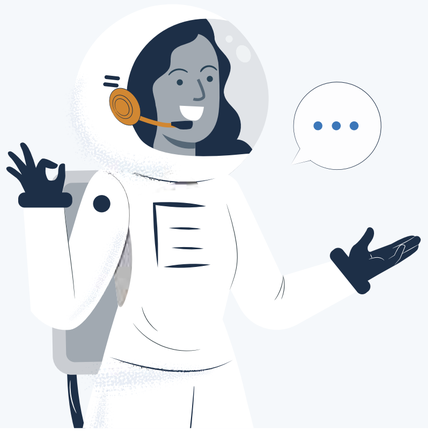
Prey también incluye monitoreo en la Dark Web para detectar si credenciales o correos institucionales han sido filtrados. Puedes tomar acción antes de que alguien intente ingresar con datos robados y cumplir con tu obligación legal de actuar y reportar ante incidentes críticos que comprometan información médica.



Implementación simple, sin infraestructura extra ni dependencia de TI interno

Prey se instala en minutos y se gestiona desde una consola web. Perfecto para clínicas y centros de salud con recursos limitados.

¿Te gustaría ver cómo funciona Prey en un entorno clínico?



Solicita una demo personalizada y conoce cómo Prey puede ayudarte a proteger tus dispositivos, resguardar información médica y cumplir con normativas como la Ley 21.663, HIPAA o FERPA.

Solicita un demo o escríbenos a sales@preyproject.com para contarnos 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**