Guía de cumplimiento con la

ley 21.663

en el sector financiero

Prey Inc.

Guía de cumplimiento con la ley 21.663 en el sector financiero

No es casualidad que el sector financiero sea el blanco favorito de los ciberataques. Tiene todo lo que los atacantes buscan: dinero, datos sensibles, y una red de sistemas críticos que, si se interrumpen, generan un impacto inmediato. Solo entre febrero y abril de 2025 se registraron en Chile más de 813 mil amenazas contra bancos y entidades similares, un salto del 53% respecto al mismo período del año anterior.

Ahora bien, muchas instituciones del rubro ya operan bajo estándares exigentes: la regulación de la CMF, los requisitos de PCI DSS, políticas ISO 27001, o frameworks propios de riesgo. La nueva Ley 21.663 no viene a reemplazar ese marco, sino a sumarle exigencias más específicas y medibles, especialmente en lo que respecta a tiempos de respuesta, trazabilidad y reporte.

Si estás en el negocio de ofrecer servicios financieros esenciales —sea banca, pagos, inversiones o seguros—, es muy probable que la ANCI te considere un Operador de Servicios Esenciales (OSE), o incluso de Operador de Importancia Vital (OIV). Esta guía está pensada precisamente para ayudarte a entender lo que eso implica y cómo prepararte sin ahogarte en burocracia.

Aumento de hackeos en Chile: alerta por ciberataques y suplantación

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

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

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

Sabías que?

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

01

¿Mi organización está obligada a cumplir?

¿Mi organización está obligada a cumplir?

Si formas parte del sistema financiero chileno —ya sea como banco, fintech, operador de medios de pago, aseguradora o entidad que maneja inversiones— lo más probable es que sí. La Ley 21.663 considera esenciales los servicios que, si fallan, pueden afectar gravemente a la ciudadanía o a la estabilidad del país. Y el sector financiero cumple con ambas condiciones.

Incluso si tu institución no ha sido designada formalmente como Operador de Servicios Esenciales (OSE) o de Importancia Vital (OIV), eso puede cambiar en cualquier momento: la ANCI tiene la facultad de evaluar y sumar nuevas entidades según su rol estratégico.

¿Aún no te designan? Eso no te deja fuera.

Como ya mencionamos, que no estés oficialmente en la lista no significa que puedas ignorar la ley. La ANCI revisa y actualiza el listado cada tres años, pero puede modificarlo antes si ocurre un incidente relevante.

El proceso que sigue la ANCI para determinar si un servicio es esencial considera tanto el impacto potencial de una interrupción como el nivel de dependencia tecnológica. ¿Qué significa esto para ti? Que si tu operación depende de plataformas críticas, redes, datacenters o software de terceros, estás dentro del radar.

Autoevaluación rápida: ¿Estás en la mira?

Pregunta	“sí” significa...
¿Gestionamos pagos, inversiones o servicios financieros esenciales?	Estás bajo criterio OSE. Regístrate en portal.anci.gob.cl
¿Una caída dejaría a más de una región sin acceso a servicios financieros?	Impacto nacional → posible OIV
¿Proveemos servicios críticos (core bancario, SaaS, cloud, data center) a bancos u OSE?	Puedes ser designado OIV por arrastre
¿Dependemos de una sola plataforma cuya caída detendría toda la operación?	Punto único de falla = foco de fiscalización inmediata
¿Manejamos datos que están protegidos por la Ley 19.628 o podrían tener consecuencias penales (Ley 20.393)?	La 21.663 refuerza tus deberes de protección y trazabilidad
¿Recibimos una encuesta, solicitud u oficio de la ANCI o CSIRT financiero?	Estás en proceso de evaluación formal. Empieza con tu SGSI hoy

A tomar en cuenta

- **3 o más “SÍ”:** Actúa ya como OSE/OIV. Las multas comienzan a aplicarse en marzo 2025.
- **1-2 “SÍ”:** Empieza a implementar controles clave y mantente atento a nuevas resoluciones.
- **0 “SÍ”:** No bajes la guardia. Las designaciones se actualizan y los riesgos no esperan.

02 Riesgos digitales críticos en el sector financiero

Riesgos digitales críticos en el sector financiero

El sector financiero no necesita hackers novatos: basta con un clic mal dado, una credencial expuesta o un endpoint sin control para abrir la puerta al caos. En esta sección revisamos los riesgos digitales más críticos para instituciones financieras, apoyándonos en datos del Data Breach Investigations Report 2025 de Verizon (DBIR), una de las fuentes más completas sobre incidentes de seguridad reales en todo el mundo.

Ransomware dirigido a core bancarios o servidores de pago

En el sector financiero, un ataque de ransomware no es solo una interrupción: puede significar la paralización de pagos, transferencias y acceso a fondos. Según el DBIR 2025, el ransomware representa el 44% de los incidentes con compromiso confirmado a nivel total, y su uso va en aumento, especialmente con herramientas más automatizadas y con objetivos bien definidos. Los atacantes no disparan al azar: van directo a sistemas centrales como core bancarios o servidores de liquidación. ¿El riesgo? Quedarte sin operar durante horas o días, con todos los focos apuntando a ti.

Robo de credenciales y fraude interno

Los atacantes ya no se esfuerzan por forzar puertas si pueden usar llaves robadas. El DBIR muestra que el 30% de las brechas financieras involucran credenciales comprometidas, lo que convierte a este vector en el más utilizado por lejos.

Pero el problema no siempre viene de fuera: el fraude interno, especialmente por personal con acceso privilegiado, también es una amenaza latente. Ya sea para mover fondos, manipular datos o extraer información crítica, las credenciales siguen siendo el eslabón más débil si no están bien protegidas ni monitoreadas.

Pérdida o exposición de dispositivos con acceso a clientes o cuentas

Uno de los riesgos más subestimados en el sector financiero es el que representan los propios dispositivos: laptops, smartphones o tablets que se usan a diario para acceder a sistemas internos o atender clientes. El DBIR 2025 revela que el 30% de los dispositivos comprometidos por malware de robo de información eran equipos con licencias empresariales.

Pero lo más preocupante es que el 46% de los sistemas comprometidos con accesos corporativos eran equipos no gestionados, que combinaban credenciales personales y laborales. Esto apunta directamente a políticas de BYOD laxas o al uso inadecuado de dispositivos corporativos fuera de lo permitido. Un dispositivo sin control ni monitoreo puede convertirse en una puerta abierta al robo de datos sensibles, sin que nadie lo note hasta que ya es demasiado tarde.

Incumplimiento de normativas (PCI, CMF, DLP)

Cumplir con normativas como PCI DSS, las exigencias de la CMF o las políticas internas de protección de datos no es solo un tema de auditorías: es una barrera concreta contra ataques reales. Según el DBIR 2025, el 74% de las brechas en el sector financiero se deben a intrusiones en sistemas, ingeniería social y ataques a aplicaciones web.

Es decir, a vectores perfectamente conocidos que pueden ser prevenidos si existen los controles adecuados. Además, aunque la motivación principal sigue siendo financiera, los ataques con fines de espionaje están aumentando. En este contexto, no cumplir las normas implica no solo exponerse a sanciones, sino renunciar a una parte clave de tu defensa. En el mundo financiero, cada control cuenta.

Fallas en trazabilidad y monitoreo de incidentes

Uno de los errores más comunes y graves es no tener visibilidad real de lo que ocurre dentro de tu red o sistemas. El DBIR muestra que en muchos casos las brechas tardan semanas o meses en detectarse, y eso ocurre principalmente por falta de monitoreo continuo y correlación de eventos.

En instituciones financieras, esta ceguera operativa impide no solo la reacción oportuna, sino también el cumplimiento de la Ley 21.663, que exige reportes rápidos (en menos de 72 horas o inmediato si es grave). Si no ves el problema, no puedes controlarlo... ni explicarlo.

03 Obligaciones principales según la ley

Obligaciones principales según la ley

Si formas parte del ecosistema financiero chileno —banco, aseguradora, entidad de pago, fintech o similar— es momento de prestar atención. La Ley 21.663 no es solo una norma más para sumar a la lista de cumplimiento: define obligaciones concretas que buscan asegurar que los servicios esenciales del país puedan anticiparse, reaccionar y recuperarse ante incidentes cibernéticos graves.

Y sí, muchas de estas obligaciones te van a sonar si ya trabajas con ISO 27001, PCI DSS o estándares CMF. Pero acá el foco no es solo tener políticas, sino demostrar capacidad operativa real frente a un ataque. A continuación, repasamos los puntos más relevantes, con énfasis en su aplicación al sector financiero:

Registro obligatorio en el portal de la ANCI

OSE : ✓ | OIV: ✓

Este es el primer paso. Todos los Prestadores de Servicios Esenciales (OSE) y de Importancia Vital (OIV) deben registrarse en el portal oficial de la ANCI. El registro habilita la supervisión, coordinación de medidas y recepción de normativas específicas por parte de la Agencia.

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

Designación de un delegado de ciberseguridad

OSE : ✓ | OIV: ✓

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

En instituciones financieras, estos roles (delegado o encargado) debe estar alineado con la gerencia de riesgos, cumplimiento y tecnología, ya que su rol cruza múltiples frentes: desde el monitoreo de amenazas hasta la preparación de informes regulatorios.

SGSI activo y documentado

OSE : ✗ | OIV: ✓

Un Sistema de Gestión de Seguridad de la Información (SGSI) no puede quedarse en la teoría. En el caso de los OIV financieros, la ley exige que sea funcional: con políticas vivas, procesos operativos y evidencia de que se aplican.

Esto incluye gestión de riesgos, controles técnicos, auditorías internas y mecanismos de respuesta. Si ya trabajas bajo ISO 27001, vas por buen camino, pero deberás adaptarlo a los tiempos y exigencias de la ANCI.

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

Reporte de incidentes: en menos de 3 horas

OSE : ✓ | OIV: ✓

Los incidentes relevantes deben notificarse al CSIRT Nacional con rapidez y trazabilidad. Esto es especialmente sensible para bancos y entidades que operan 24/7.

El proceso incluye tres etapas:

1. **Alerta inicial en máximo 3 horas** desde la detección.
2. **Informe detallado en 72h** (24h en el caso de OIV) con evaluación de impacto, IoC, y plan de acción.
3. **Informe final en 15 días corridos.**

El reporte usa formato XML y taxonomía ANCI.
Decreto N° 295 | Resolución N° 7/2025

Auditorías, análisis de riesgos y simulacros

OSE : ✗ | OIV: ✓

Los OIV deben someterse a auditorías periódicas, tanto internas como externas, así como a evaluaciones de riesgo y simulacros de incidentes.

Para el sector financiero, esto se traduce en pruebas de continuidad de pagos, reacción ante brechas de datos, o fallas de autenticación. Todo debe quedar documentado y disponible ante una fiscalización.

Planes de continuidad operacional y ciberseguridad

OSE : ✗ | OIV: ✓

La ley exige que los OIV cuenten con planes actualizados que garanticen la continuidad de los servicios críticos durante un incidente. En la banca, esto puede significar mantener activos los sistemas de compensación, canales digitales o incluso call centers.

Estos planes deben actualizarse al menos cada dos años y estar certificados según lo indicado en el artículo 28 de la ley.

Recomendamos:
Crea tu plan de respuesta a incidentes de ciberseguridad

Medidas para reducir impacto y propagación de incidentes

OSE : ✗ | OIV: ✓

La ley obliga a tomar acciones inmediatas para contener incidentes. En una institución financiera esto puede implicar revocar accesos, aislar segmentos de red o activar backups protegidos. No basta con “investigar”: hay que reaccionar en tiempo real.

Certificaciones de respaldo

OSE : ✗ | OIV: ✓

Los OIV deben contar con certificaciones como ISO 27001 que avalen la efectividad de su SGSI y sus planes de continuidad. Aunque los OSE no están obligados a certificarse, **la ANCI se basa en estándares internacionales** como ISO, NIST y CIS para sus auditorías.

En el mundo financiero, donde ya se exige ISO o PCI en muchos casos, esto no es nuevo, pero ahora también es una carta ante el regulador nacional.

Notificación a potenciales afectados

OSE : ✗ | OIV: ✓

Si el incidente compromete datos personales o servicios críticos, y la ANCI lo instruye, la organización debe informar a los usuarios o clientes afectados. En servicios financieros, esto puede involucrar cuentas, identificadores o transacciones expuestas.

Programas de capacitación y campañas de ciberhigiene

OSE : ✗ | OIV: ✓

Uno de los focos más relevantes (y menos técnicos) es la formación de tu equipo. Los OSE y OIV deben implementar entrenamientos continuos y campañas de buenas prácticas. Simulacros de phishing, talleres de gestión de contraseñas y políticas claras de uso de dispositivos son esenciales para reducir errores humanos.

Cumplimiento de normativas técnicas ANCI o sectoriales

OSE : ✓ | OIV: ✓

Por último, todas las instituciones deben adherirse a las normativas técnicas que emita la ANCI y, en el caso del sector financiero, también las que dicte la **CMF**. La buena noticia: muchas de estas medidas ya están contempladas en estándares como PCI DSS, ISO 27001 o los propios manuales de continuidad operativa de la banca.

La clave es integrarlas con los nuevos requerimientos de trazabilidad y reporte exigidos por la ley.

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

04

Qué pasa si no cumples con la Ley 21.663?

Qué pasa si no cumples con la Ley 21.663?

En ciberseguridad, no basta con decir “lo estamos viendo”. La Ley 21.663 clasifica el incumplimiento en tres niveles: leve, grave y gravísimo, según el impacto y la naturaleza de la falta. Y en el caso del sector financiero, donde hay estándares regulatorios adicionales y obligaciones frente a la CMF, el margen de error es aún más estrecho.

Las consecuencias no se limitan a multas. El incumplimiento también puede provocar la pérdida de certificaciones clave como **PCI DSS, ISO 27001 o SOC 2**, que son requisitos para operar en ciertos mercados financieros o mantener alianzas con bancos, emisores y adquirentes. En otras palabras, no cumplir puede cerrar puertas y frenar tu operación.

Tipo de infracción	Definición breve	Multa máxima (OSE)	Multa máxima (OIV)
Leve	Retrasos o fallas menores sin impacto crítico.	5.000 UTM	10.000 UTM
Grave	No aplicar estándares, omitir reportes críticos, obstrucción.	10.000 UTM	20.000 UTM
Gravísima	Incidentes graves no gestionados o reincidencias.	20.000 UTM	40.000 UTM

Tipos de infracciones según el artículo 38

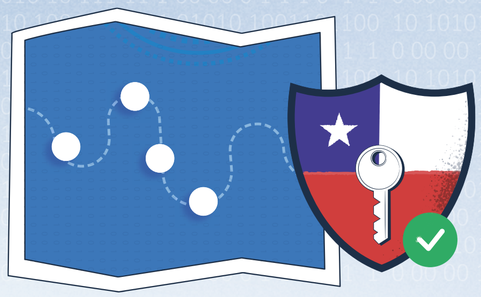
Categoría Infracciones	Infracciones OSE	Infracciones OIV
Infracciones Leves	• No responder a tiempo requerimientos no críticos de la ANCI. • Incumplir instrucciones menores. • Otras faltas no clasificadas como graves.	• No mantener trazabilidad de controles aplicados. • No reportar simulacros o revisiones. • No implementar campañas de concientización. • No designar delegado. • No contar con certificaciones de planes ni de SGSI.
Infracciones Graves	• No implementar estándares de ANCI o CMF. • Presentar información falsa. • No reportar un incidente relevante. • Obstaculizar el trabajo de ANCI. • Reincidir en faltas leves.	• No contar con un SGSI operativo. • No aplicar ni ejecutar planes de continuidad. • No notificar a afectados por una brecha. • No contener amenazas activas. • Reincidir en infracciones leves.
Infracciones Gravísimas	• Falsificar información clave en medio de un incidente. • No obedecer instrucciones durante una crisis de seguridad relevante. • Ocultar información sobre un incidente grave. • Reincidir en infracciones graves.	• No aplicar medidas de contención ante incidentes críticos. • Reincidir en infracciones graves dentro del año.

¿Qué agrava una sanción?

La reincidencia, el impacto económico de la brecha, la exposición pública, el número de afectados, o simplemente el tamaño de la institución, son factores que pueden escalar la multa. Las entidades financieras, por su peso estratégico y la cantidad de datos sensibles que manejan, están bajo especial escrutinio.

Imagina una fintech que omite reportar un ciberataque que expone datos de clientes. Si no toma medidas de contención y el incidente se extiende a otros servicios o afecta la disponibilidad de pagos, la falta pasa de grave a gravísima, con multas que pueden superar los mil millones de pesos y el riesgo de quedar fuera de operación, ya sea por resolución de la ANCI o por pérdida de certificaciones exigidas por aliados estratégicos.

05



Pasos prácticos para cumplir con la Ley 21.663

Pasos prácticos para cumplir con la Ley 21.663

Cumplir con la Ley 21.663 no significa reinventar tu operación ni empezar desde cero. Si ya trabajas con estándares como PCI DSS, ISO 27001 o regulaciones de la CMF, el camino ya está avanzado. Lo clave es adaptar lo que ya tienes a los requerimientos específicos de trazabilidad, tiempos y roles que exige la ley.

Mapea tus obligaciones regulatorias actuales (CMF, PCI, ISO)
Antes de moverte, revisa lo que ya estás obligado a cumplir. ¿Tienes controles PCI activos? ¿Te audita la CMF? ¿Tu SGSI cubre continuidad y ciberresiliencia? Este diagnóstico te permite ver qué ya tienes cubierto y qué debes reforzar para cumplir con la Ley 21.663 sin duplicar esfuerzos ni recursos.

Designa al delegado de ciberseguridad formalmente y documenta su rol
Este no es un “encargado TI honorario”. Debe ser una figura visible, con respaldo de la alta dirección, y con funciones claras: desde canalizar reportes hacia la ANCI hasta coordinar respuestas internas y monitorear el cumplimiento del SGSI. Formaliza su rol por escrito y asegúrate de que tenga tiempo y recursos.

Adapta tu SGSI: que cubra controles críticos, trazabilidad, monitoreo y respuesta Si ya trabajas con ISO 27001, el SGSI es tu columna vertebral. Pero ahora debe ser más ágil y práctico: debe registrar evidencia de acciones, responder a incidentes en tiempos exigentes (3h/72h), y demostrar trazabilidad. No basta con tenerlo: hay que activarlo y alinearlo con el enfoque operativo de la ley.

Integra herramientas que den visibilidad y respuesta en tiempo real
No puedes proteger lo que no ves. Necesitas soluciones que te alerten si un dispositivo sale del país, si hay un intento de intrusión o si alguien accede fuera de horario. EDR, MDM, SIEM y monitoreo continuo te permiten detectar y actuar antes de que un incidente escale.

Define y prueba tu plan de continuidad operativa (PCO)

Si eres un OIV, este plan es obligatorio, pero para los OSE también es una muy buena idea. Define qué servicios no pueden detenerse, cómo restaurarlos rápidamente y qué hacer si tus sistemas críticos caen. Luego, prueba ese plan con simulacros realistas: no esperes a una crisis para ver si funciona.

Prepara flujos de reporte en menos de 3 horas y prueba simulacros

La Ley 21.663 exige notificar incidentes relevantes al CSIRT en un máximo de 3 horas. Para lograrlo, necesitas saber exactamente quién reporta, qué se informa y cómo se recopilan los datos. Armar ese flujo y probarlo en ejercicios internos te evita correr en círculos cuando el reloj ya está en contra.

Conecta cumplimiento con auditorías internas y continuidad de negocio

No trates el cumplimiento como una isla. Tus procesos de auditoría interna, gestión de riesgos y planes de continuidad deben conversar entre sí. Así podrás usar evidencia ya existente para demostrar cumplimiento, identificar brechas antes de una fiscalización y reforzar lo que realmente importa: seguir operando, pase lo que pase.

Herramientas tecnológicas recomendadas para el sector financiero

Ya no basta con tener un antivirus y un firewall, pensar que basta con eso es dejar las puertas abiertas a todo tipo de desastres cibernéticos. Desde oficinas centrales hasta notebooks de ejecutivos en terreno, cada dispositivo puede ser una puerta de entrada para un ataque. Y con regulaciones como la CMF, PCI DSS e ISO 27001 sobre la mesa, tu stack de seguridad no puede quedarse corto.

Aquí te mostramos las herramientas que no pueden faltar si trabajas con datos financieros, canales de pago o infraestructura crítica.

Además, verás por qué el Data Breach Investigations Report 2025 (DBIR) las respalda con datos que no conviene ignorar:

Categoría	Descripción de la herramienta	Por qué importa	Ejemplos
MDM (monitoreo de dispositivos)	Monitorea laptops y móviles, aplica políticas, rastrea, bloquea o borra datos de forma remota.	El **46% de sistemas** comprometidos no eran manejados y poseían datos personales y de negocios.	Prey , Microsoft Intune, Jamf Pro
Gestión de parches	Automatiza actualizaciones de sistemas y software, prioriza vulnerabilidades críticas.	**20% de los incidentes** aprovecharon software vulnerable.	Automox, Ivanti Neurons, WSUS
Protección de endpoints (AV + EDR)	El antivirus detiene malware conocido; el EDR detecta comportamientos sospechosos y aísla amenazas.	El ransomware sigue al alza: **44% de las brechas** lo incluyeron.	SentinelOne, CrowdStrike Falcon
SIEM / UEBA	Centraliza logs y detecta anomalías usando análisis de comportamiento.	**60% de los incidentes** incluyen fallas humanas: este sistema los identifica.	Splunk, Wazuh, Microsoft Sentinel
Backups 3-2-1	Copias locales + nube, con inmutabilidad y pruebas regulares de restauración.	Sin backups verificados no hay plan B viable.	Veeam, Acronis Cyber Protect
Gestor de contraseñas	Guarda claves cifradas, evita repetición y facilita MFA.	Las credenciales siguen siendo la llave maestra del **31% de las brechas.**	Bitwarden, 1Password
IAM / CABS	Administra identidades, roles y accesos, aplica MFA y políticas Zero Trust.	Aplica mínimo privilegio: nadie accede a más de lo necesario.	Azure AD, Okta, ForgeRock
Firewall perimetral / cloud	Segmentan tráfico, protegen VPNs y aplican reglas Zero Trust.	Dispositivos de red mal protegidos fueron el inicio de ataques en **22% de los casos.**	Palo Alto Networks, Zscaler

Herramientas complementarias (pero igual de críticas)

En un sector con tanta exposición como el financiero, estas herramientas no son lujo, son blindaje. Detectan, educan, automatizan y cierran brechas que un atacante explota en minutos.

Categoría	Descripción	Por qué importa	Ejemplos
DLP (Prevención de pérdida de datos)	Identifica, monitorea y protege datos sensibles en tránsito, uso y almacenamiento.	Evita fugas de datos críticos por errores o malas prácticas.	Endpoint Protector, Forcepoint, Microsoft Purview
Simuladores de phishing y concientización	Entrena a equipos con escenarios reales y mide su respuesta.	60% de incidentes involucran usuarios: entrenarlos no es opcional.	KnowBe4, Phished, Hook Security
SOAR (Respuesta automatizada)	Orquesta acciones ante incidentes: desde aislar equipos hasta bloquear accesos.	Usuarios = 60% de las brechas. Entrena y mide la mejora.	Cortex XSOAR, Splunk SOAR
Automatización de compliance y evidencias	Mapea controles legales y técnicos, genera reportes automáticos para ANCI o auditorías.	Ahorra horas de documentación y entrega reportes listos.	Vanta, Drata, Hackmetrix
IDS/IPS	Monitorea tráfico de red y bloquea intrusiones en tiempo real.	Detecta ataques antes de que lleguen al endpoint.	Snort, Suricata, Cisco Secure IPS
Análisis de vulnerabilidades	Escanea sistemas, prioriza riesgos y sugiere acciones.	El 20% de las brechas usó vulnerabilidades conocidas.	Nessus, Qualys VMDR, Rapid7 InsightVM

Escenario realista para no morir en el intento.

1. Prioriza herramientas donde el impacto regulatorio sea mayor (ej: pérdida de datos bancarios = multas + pérdida de certificaciones).
2. Integra MDM, SIEM y SOAR para tener visibilidad, trazabilidad y respuesta automática en un solo flujo.
3. Simula incidentes como filtraciones de datos o caídas de sistema de pagos. Si no lo puedes probar hoy, tampoco lo vas a poder defender mañana.

> Bonus: documenta todo. Desde la capacitación hasta los reportes automáticos. La ANCI, la CMF... y tu auditor de PCI lo agradecerán.

06 Buenas prácticas en procesos y personas

Buenas prácticas en procesos y personas

La tecnología sola no basta. Un buen programa de ciberseguridad en el sector financiero también se sostiene en procesos bien definidos y personas que saben lo que deben hacer. Desde clasificar los datos hasta coordinar áreas clave, estas buenas prácticas ayudan a prevenir errores, fortalecer la respuesta y demostrar cumplimiento ante cualquier fiscalización.

Clasificación y protección de datos según nivel de sensibilidad No toda la información debe tratarse igual. Identifica y etiqueta tus activos según su nivel de sensibilidad: datos públicos, internos, confidenciales o críticos, es decir, lo que serían datos como cuentas bancarias, claves API, PII.

Esto te permite aplicar controles adecuados (como cifrado o segmentación) y crear una matriz de riesgo más precisa. Así sabrás qué proteger primero y cómo responder si algo se ve comprometido.

Políticas internas claras para uso de dispositivos, teletrabajo y acceso remoto Define reglas simples y aplicables: quién puede conectarse desde dónde, con qué dispositivos, y bajo qué condiciones. Una política efectiva evita que tus sistemas sean vulnerables por accesos desde redes inseguras o por el uso personal de equipos corporativos sin control. hardcodeados.

Algunas fundamentales para este contexto son:

- **Política de uso aceptable:** Define lo que se puede y no se puede hacer con los equipos y redes de la empresa.
- **Política de teletrabajo:** Establece los requisitos de seguridad para trabajar desde casa (VPN, MDM, cifrado).
- **Política de control de acceso:** Indica cómo se asignan permisos y se controla el ingreso a sistemas sensibles.
- **Política BYOD:** Regula el uso de dispositivos personales para tareas laborales, incluyendo medidas mínimas.

Simulacros frecuentes de incidentes (phishing, denegación de servicio, pérdida de activos) La teoría está bien, pero la práctica salva el día. Realizar simulacros te permite probar si los planes realmente funcionan. Puedes simular ataques de phishing para medir la reacción de los usuarios, cortes de servicios clave o incluso la pérdida de un laptop con información crítica. Además de entrenar al equipo, estos ejercicios generan evidencias útiles para auditorías y revisiones internas.

Integración del área de cumplimiento, TI y auditoría interna

La ciberseguridad no es solo cosa del área técnica. Para que las medidas sean efectivas y sostenibles, TI debe trabajar en conjunto con cumplimiento y auditoría. Esto garantiza que los controles estén alineados con normativas como la Ley 21.663, PCI DSS e ISO 27001, que los riesgos se gestionen de forma integral y que la trazabilidad esté cubierta desde la prevención hasta la respuesta.

El delegado de ciberseguridad en instituciones financieras

En el sector financiero, el delegado de ciberseguridad no puede ser “alguien que sabe de TI”. Necesitas a una persona con experiencia real en gestión de riesgos, cumplimiento normativo y respuesta a incidentes. Si no tienes ese perfil dentro del equipo, puedes considerar externalizar el rol con un especialista independiente o un proveedor MSSP con las competencias adecuadas.

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.

Debe tener autonomía, respaldo de la alta dirección y contacto directo con la ANCI

No puede ser un rol simbólico ni un puesto sin poder real. El delegado necesita autonomía para actuar, recursos para implementar medidas y un canal directo con la alta dirección y la ANCI. Su voz debe pesar en las decisiones clave y contar con el respaldo necesario para detener procesos si hay riesgo.

Rol clave en la trazabilidad, gestión de incidentes y control documental

Cuando ocurre un incidente, todas las miradas apuntan al delegado. Debe activar los flujos de respuesta, documentar cada acción y asegurar que todo quede registrado para reportes y auditorías. También es quien mantiene actualizada la evidencia de cumplimiento, lidera simulacros y gestiona la trazabilidad de las decisiones que afectan la seguridad.

Debe ser designado formalmente por el representante legal de la entidad

La designación no puede quedar en un correo o en un acta informal. Según la Ley 21.663, el delegado debe ser nombrado oficialmente mediante un acto administrativo firmado por el representante legal. Esta formalidad garantiza su legitimidad ante la ANCI y establece claramente su rol y responsabilidades dentro de la organización.

07

Cómo Prey puede ayudarte a cumplir con la Ley 21.663 en el sector financiero

Cómo Prey puede ayudarte a cumplir con la Ley 21.663 en el sector financiero

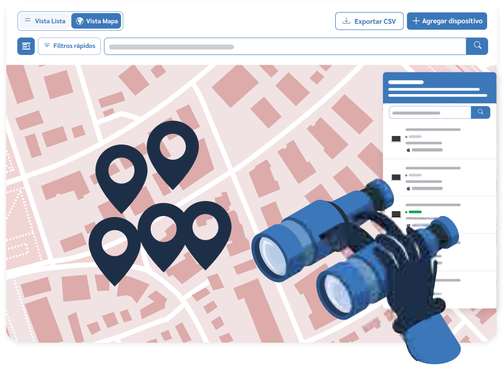
En un entorno como el financiero, donde un dispositivo comprometido puede significar acceso directo a datos sensibles, cuentas de clientes o sistemas críticos, Prey ofrece un set de soluciones concretas para cumplir con la Ley 21.663 sin complejidades innecesarias.

Su plataforma centraliza la gestión, protección y monitoreo de endpoints, permitiendo visibilidad, respuesta rápida y generación de evidencia para auditorías —todo desde una interfaz intuitiva que no requiere un equipo técnico especializado.

Detección temprana y reacción ante incidentes

¿Un dispositivo cambia de red de forma sospechosa? ¿Se activa fuera de horario? Prey puede notificarte automáticamente con alertas, activar geocercas y ejecutar acciones como el bloqueo inmediato de pantalla, mensajes al usuario o alarmas disuasivas. Todo esto permite contener incidentes en minutos y documentar la respuesta ante eventos como robos, pérdidas o accesos no autorizados.

Visibilidad y control de activos en sucursales y remoto



Prey te permite tener la vista total de tus laptops, tablets y móviles, sin importar si están en una oficina, sucursal o en casa del ejecutivo. Desde un panel unificado puedes geolocalizar dispositivos, asignarlos por área o función (riesgo operativo, tesorería, cumplimiento), aplicar políticas y administrar diferentes sistemas operativos como Windows, macOS o Android. Ideal para mantener el control de flotas móviles y ejecutivos que viajan.

Protección activa de datos confidenciales

Una laptop perdida con acceso a banca digital o sistemas core no puede quedar expuesta. Prey permite ejecutar borrado remoto, restablecer configuraciones de fábrica y activar cifrado (como BitLocker en Windows) para evitar filtraciones. Estas funciones son clave para cumplir con exigencias de confidencialidad del cliente, PCI DSS y la Ley 21.663.

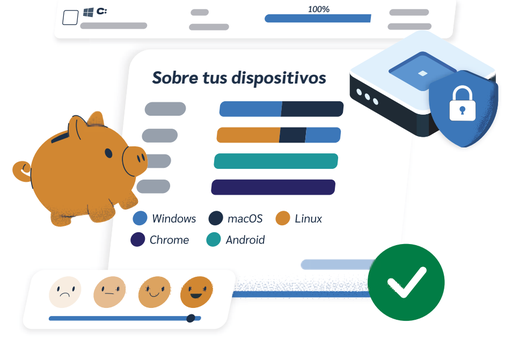
Evidencia y trazabilidad listas para auditoría

Cada acción que se ejecuta —desde un bloqueo remoto hasta un cambio de red— queda registrada en el Audit Log. Este historial detallado facilita las auditorías internas, externas y las de la ANCI, demostrando trazabilidad, proactividad y cumplimiento. También permite reconstruir incidentes en caso de investigación.

Dark Web Monitoring para proteger tus credenciales

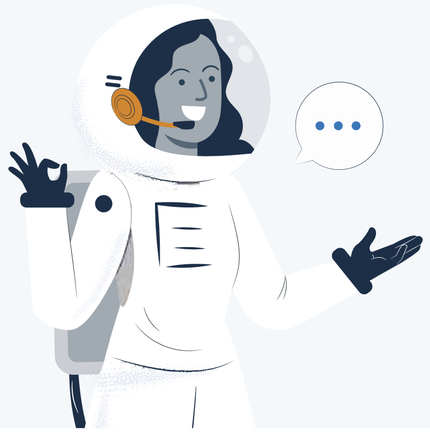
Prey incluye monitoreo en la Dark Web que detecta filtraciones de credenciales asociadas a tu dominio. En el sector financiero, donde el robo de credenciales es uno de los vectores más comunes, esta funcionalidad te permite actuar antes de que un atacante las use, cumpliendo además con tu deber de prevención y notificación.

Ideal para PYMEs financieras sin un SGSI completo



¿Aún no tienes un SGSI completo tipo ISO 27001? No hay problema. Prey cubre varios controles clave exigidos por la ley: gestión de activos, monitoreo, respuesta, visibilidad y evidencia. Es una alternativa accesible, rápida de implementar y compatible con los marcos más exigentes, sin que tengas que sobredimensionar tu equipo o presupuesto.

¿Quieres ver cómo Prey se adapta a tu institución financiera?



Solicita una demo personalizada para conocer cómo Prey puede ayudarte a cumplir con la Ley 21.663 y otras normativas relevantes como PCI DSS, ISO 27001 o los estándares de la CMF.

Solicita un demo o escríbenos a sales@preyproject.com para que podamos ayudarte según tu caso y tamaño de operación.

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**

Prey Spa. © Santiago, RM Chile

Todos los derechos reservados. La aplicación Prey, el logo y su marca son marcas registradas de Prey Inc.