Checklist de cumplimiento de la Ley Marco de Ciberseguridad

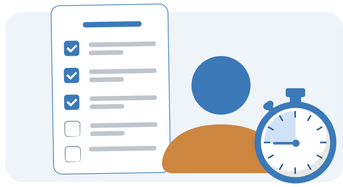
Checklist de cumplimiento de la Ley Marco de Ciberseguridad

En Prey sabemos que la ciberseguridad debería sentirse tan clara como encender la linterna del celular, no como descifrar un manual de 300 páginas. Hemos preparado este documento como una hoja de ruta transversal para cualquier organización—pública o privada, grande o pequeña—que deba alinearse con la Ley Marco de Ciberseguridad (21.663) de Chile. Funciona como código de seguimiento rápido posterior a nuestra guía y concentra, en un único formato accionable:

El presente documento sirve

- **Auto-chequeo express:** cuatro preguntas clave para determinar si podrías ser designado Operador de Servicio Esencial (OSE) o de Importancia Vital (OIV).
- **Primeros pasos formales ante la ANCI:** registro en el portal oficial y habilitación de canales de reporte.
- **Diez hitos operativos:** desde el diagnóstico inicial y la selección de un marco de control (ISO 27001 / NIST CSF) hasta la documentación final, con campos para responsable, fecha objetivo y evidencia.

Cómo utilizar esta herramienta



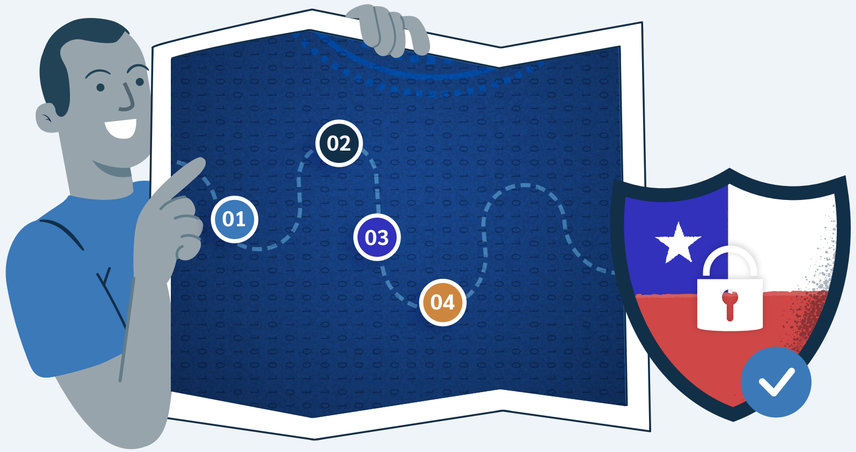
1. **Asigna responsables** y plazos realistas a cada ítem.

2. **Integra la lista** a tu sistema de gestión de proyectos o SGSI.

3. **Adjunta evidencias** (informes, capturas, actas) para demostrar cumplimiento en auditorías.

4. **Revisa y actualiza** periódicamente: la normativa y tu entorno de riesgos pueden cambiar.

	Paso	Responsable	Fecha objetivo	Anotaciones / Evidencia:
☐	**Evaluar estatus OSE/OIV** • Revisar art. 4° de la Ley 21.663 y el impacto de una interrupción (LMS, redes, data center)			**Auto-chequeo express:** • ¿Prestamos alguno de los ocho servicios esenciales (salud, energía, transporte, etc.)? • Si nuestra plataforma cae, ¿afecta la salud, seguridad o economía de la comunidad? • ¿Gestionamos infraestructura digital crítica (data center, red académica, servicios cloud) a clientes OSE/OIV? • ¿Gestionamos datos cuyo robo obligaría a notificar según Ley 19.628/21.719 o expone riesgo penal Ley 20.393? • ¿Recibimos fondos públicos o subvenciones significativas? **→ Si se responde "sí" a ≥ 2 preguntas, iniciar proceso de clasificación OSE/OIV.**
☐	**Nombrar Delegado/a de Ciberseguridad c**on autoridad y presupuesto			Resolución interna / carta de nombramiento
☐	**Registrar la institución en el portal ANCI** (portal.anci.gob.cl) y validar credenciales de reporte			Registrarse en portal.anci.gob.cl con clave única del contacto de la empresa con la ANCI Captura de pantalla del registro aprobado
☐	**Diagnóstico rápido** de brechas ISO 27001 / NIST y criticidad de activos			Realizar un inventario de activos y matriz de riesgos de tu situación actual
☐	**Elegir marco** (ISO 27001 o NIST CSF) y mapear controles "Sí / No / Parcial"			Mapa de controles con responsables asignados
☐	**Plan por fases** con metas trimestrales (controles mínimos → certificación → mejora)			Roadmap aprobado por Dirección
☐	**Seleccionar herramientas base** (MDM, AV/EDR, Firewall, backup 3-2-1, gestor de contraseñas + MFA, etc)			Puedes tomar como benchmark según el mapa de controles técnicos requeridos del paso 5 Licencias adquiridas y desplegadas
☐	**Automatizar alertas** y panel único de monitoreo (MDM, EDR, Firewall, SIEM)			Dashboard operativo con reglas de severidad
☐	**Entrenar al personal** (phishing simulado, micro-lecciones, inducción)			Definir un roadmap de capacitación Registro de asistencia y resultados de tests
☐	**Definir planes de continuidad** (Procesos críticos de la institución)			Plan BCP/DR validado y publicado
☐	**Ejecutar simulacros** semestrales (ransomware, corte eléctrico, interrupciones de infraesctura)			Reporte de simulacro con tiempos D/C/R
☐	**Documentar todo** en repositorio accesible y versionado			Carpeta SGSI completa + evidencias auditables

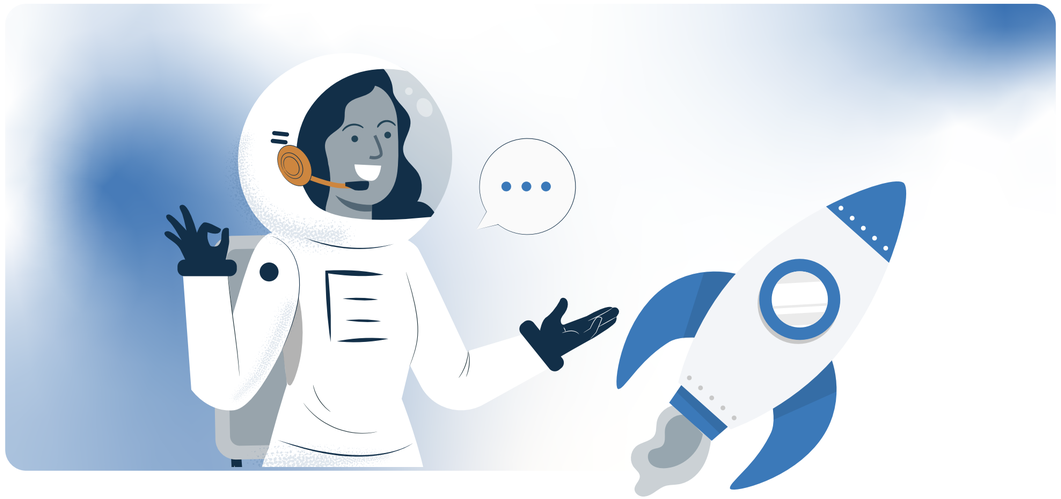


Próximos pasos

Al completar este checklist, tu organización habrá recorrido los hitos mínimos que exige la Ley 21.663 para cualquier entidad que preste servicios críticos o aspire a certificar su Sistema de Gestión de la Seguridad de la Información (SGSI). Mantén la lista viva—revísala en cada comité de ciberseguridad, ajusta plazos cuando cambien las prioridades y agrega controles adicionales conforme evolucione la regulación o el negocio.

En Prey vemos la ciberresiliencia como un viaje continuo, no un destino fijo. Vuelve a esta lista cada vez que tu negocio crezca, tu tecnología cambie o la normativa evolucione. Y si necesitas una mano extra—ya sabes dónde encontrarnos.

¿Listo para llevar tu seguridad al siguiente nivel?



Agenda una demo personalizada con nuestro equipo y descubre cómo Prey puede ayudarte a cumplir la Ley 21.663 sin complicaciones ni presupuestos elevados.

Escríbenos a sales@preyproject.com

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 ofrecerte apoyo.

preyproject.com