GUÍA BASE DE PREPARACIÓN

Ley N° 21.663

Matriz práctica para identificar brechas, responsablesy próximospasos

Incluye autodiagnóstico, ruta de reporte de incidentes y plan inicial de 30 días.

Preparación útil, evidencia verificable.

Servicios Integrales en Ciberseguridad

EDICIÓN	JULIO 2026
USO	AUTODIAGNÓSTICO INICIAL

Cómo usar esta guía

Esta guía permite realizar una revisión inicial y ordenada del nivel de preparación de la organización frente a la Ley N° 21.663.

1 Confirma el alcance

Determina si la organización presta un servicio esencial y revisa si fue calificada como Operador de Importancia Vital (OIV).

2 Evalúa cada control

Marca el estado real y registra la evidencia disponible. Evita responder solo por percepción.

3 Asigna responsables

Cada brecha debe quedar asociada a una persona, una fecha y un resultado esperado.

4 Prioriza lo crítico

Comienza por reporte de incidentes, continuidad del servicio, activos críticos y dependencias clave.

Antes de comenzar

Prestadores de servicios esenciales

Tienen deberesgeneralespermanentesy deben reportar incidentes con efectos significativos.

Operadores de Importancia Vital (OIV)

Son entidades calificadas por la ANCI y deben cumplir obligaciones adicionales, entre ellas designar un delegado de ciberseguridad.

Estándares técnicos

La ANCI inició en mayode 2026 la consulta pública de los estándares básicos obligatorios.
Esta guía debe actualizarse cuando se publique su versión definitiva.

ESCALA SUGERIDA DE MADUREZ

NO INICIADO	EN DESARROLLO	IMPLEMENTADO	VERIFICADO
No existe una medida formal.	Hay avances,pero falta completar o probar.	La medida opera y tiene evidencia.	La medida fueprobada,revisada o auditada.

Uso orientativo. Esta guía no reemplaza una revisión legal, regulatoria ni sectorial específica.

MATRIZ

Autodiagnóstico 1 | Alcance y gobierno

LEY 21.663

Marca el estado real,registra la evidencia disponible y asigna un responsable con fecha.

N°	Punto de control	Qué verificar	Evidencia esperada	Estado	Responsable / fecha
1	**Alcance legal**	Confirmar si la organización presta actividades calificadas como servicios esenciales conforme al artículo 4.	Análisis de aplicabilidad aprobado por gerencia o asesoría jurídica.	• Cumple • Cumple parcialmente • No cumple • En implementación • No aplica	**Responsable:** _____ **Fecha:** _____
2	**Calificación OIV**	Revisar si la entidad figura en una nómina final de OIV publicada por la ANCI.	Resolución aplicable y respaldo de la revisión.	• Cumple • Cumple parcialmente • No cumple • En implementación • No aplica	**Responsable:** _____ **Fecha:** _____
3	**Gobierno ejecutivo**	Definir quién toma decisiones, aprueba prioridades y recibe escalamiento de riesgos e incidentes.	Comité, acta, política o matriz RACI.	• Cumple • Cumple parcialmente • No cumple • En implementación • No aplica	**Responsable:** _____ **Fecha:** _____
4	**Encargado de reportes**	Designar y mantener actualizado el responsable operativo de reportar incidentes.	Documento de designación y datos de contacto vigentes.	• Cumple • Cumple parcialmente • No cumple • En implementación • No aplica	**Responsable:** _____ **Fecha:** _____
5	**Delegado de ciberseguridad - OIV**	Formalizar el delegado con reporte directo, independencia funcional y capacidad para representar a la institución ante la ANCI.	Documento formal, organigrama, perfil y acreditación.	• Cumple • Cumple parcialmente • No cumple • En implementación • No aplica	**Responsable:** _____ **Fecha:** _____
6	**Política institucional**	Aprobar una política que establezca objetivos, roles, responsabilidades y criterios de cumplimiento.	Política vigente, aprobada y comunicada.	• Cumple • Cumple parcialmente • No cumple • En implementación • No aplica	**Responsable:** _____ **Fecha:** _____
7	**Seguimiento de cumplimiento**	Revisar periódicamente avances, brechas, riesgos y compromisos regulatorios.	Tablero, minutas y plan de mejora.	• Cumple • Cumple parcialmente • No cumple • En implementación • No aplica	**Responsable:** _____ **Fecha:** _____

MATRIZ

Autodiagnóstico 2 | Riesgos y activos

LEY 21.663

Marca el estado real,registra la evidencia disponible y asigna un responsable con fecha.

N°	Punto de control	Qué verificar	Evidencia esperada	Estado	Responsable / fecha
1	**Servicios y procesos críticos**	Identificar los servicios esenciales y procesos necesarios para mantener su continuidad.	Mapa de servicios, procesos y dependencias.	• Cumple • Cumple parcialmente • No cumple • En implementación • No aplica	**Responsable:** _____ **Fecha:** _____
2	**Inventario de activos**	Registrar sistemas, redes, aplicaciones, datos, identidades, infraestructura y servicios en la nube vinculados a lo crítico.	Inventario actualizado, propietario y criticidad.	• Cumple • Cumple parcialmente • No cumple • En implementación • No aplica	**Responsable:** _____ **Fecha:** _____
3	**Dependencias y terceros**	Identificar proveedores cuya falla o compromiso pueda afectar la continuidad o seguridad.	Mapa de terceros, contratos y evaluación de criticidad.	• Cumple • Cumple parcialmente • No cumple • En implementación • No aplica	**Responsable:** _____ **Fecha:** _____
4	**Evaluación de riesgos**	Analizar amenazas, vulnerabilidades, impacto y probabilidad sobre servicios y activos críticos.	Matriz de riesgos con metodología definida.	• Cumple • Cumple parcialmente • No cumple • En implementación • No aplica	**Responsable:** _____ **Fecha:** _____
5	**Plan de tratamiento**	Asignar controles, presupuesto, responsables y plazos a los riesgos no aceptados.	Plan de tratamiento aprobado y trazable.	• Cumple • Cumple parcialmente • No cumple • En implementación • No aplica	**Responsable:** _____ **Fecha:** _____
6	**Respaldo y recuperación**	Definir copias de seguridad, protección, restauración y pruebas periódicas.	Política de respaldo y evidencias de restauración.	• Cumple • Cumple parcialmente • No cumple • En implementación • No aplica	**Responsable:** _____ **Fecha:** _____
7	**Monitoreo y registros**	Mantener visibilidad sobre eventos, accesos, cambios y señales de compromiso.	Registros centralizados, alertas y retención definida.	• Cumple • Cumple parcialmente • No cumple • En implementación • No aplica	**Responsable:** _____ **Fecha:** _____

MATRIZ

Autodiagnóstico 3 | Incidentes

LEY 21.663

Marca el estado real,registra la evidencia disponible y asigna un responsable con fecha.

N°	Punto de control	Qué verificar	Evidencia esperada	Estado	Responsable / fecha
1	**Criterio de incidente significativo**	Definir cómo reconocer incidentes que puedan afectar continuidad, personas, sistemas, accesos no autorizados o datos personales.	Matriz de clasificación y ejemplos internos.	• Cumple • Cumple parcialmente • No cumple • En implementación • No aplica	**Responsable:** _____ **Fecha:** _____
2	**Procedimiento de respuesta**	Establecer detección, análisis, contención, erradicación, recuperación y cierre.	Plan de respuesta, playbooks y lista de contactos.	• Cumple • Cumple parcialmente • No cumple • En implementación • No aplica	**Responsable:** _____ **Fecha:** _____
3	**Reporte a la ANCI**	Preparar el flujo para alerta temprana, segundo reporte, plan de acción OIV e informe final.	Procedimiento, accesos y formato de recopilación de datos.	• Cumple • Cumple parcialmente • No cumple • En implementación • No aplica	**Responsable:** _____ **Fecha:** _____
4	**Preservación de evidencia**	Definir cómo resguardar registros, indicadores, cronología y decisiones durante el incidente.	Procedimiento de evidencia y bitácora.	• Cumple • Cumple parcialmente • No cumple • En implementación • No aplica	**Responsable:** _____ **Fecha:** _____
5	**Continuidad y recuperación**	Establecer prioridades, RTO, RPO, alternativas operativas y recuperación de servicios.	BCP/DRP vigentes y aprobados.	• Cumple • Cumple parcialmente • No cumple • En implementación • No aplica	**Responsable:** _____ **Fecha:** _____
6	**Ejercicios y pruebas**	Realizar simulaciones técnicas y ejecutivas para validar tiempos, roles y comunicaciones.	Informes de ejercicios y acciones correctivas.	• Cumple • Cumple parcialmente • No cumple • En implementación • No aplica	**Responsable:** _____ **Fecha:** _____
7	**Lecciones aprendidas**	Analizar causas, fallas de control, impactos y mejoras después de cada incidente o ejercicio.	Informe post incidente y seguimiento.	• Cumple • Cumple parcialmente • No cumple • En implementación • No aplica	**Responsable:** _____ **Fecha:** _____

FLUJO

Ruta de reporte de incidentes

LEY 21.663

Aplica a incidentes o ciberataques que puedan tener efectos significativos. El plazo se cuenta desde que la institución toma conocimiento.

1	2	OIV SI EL SERVICIO ES AFECTADO	OIV PLAN DE ACCIÓN	3
Máximo 3 horas	**Máximo 72 horas**	**Máximo 24 horas**	**Máximo 7 días corridos**	**Máximo 15 días corridos**
Identificación, contacto, fecha/hora, indicios y activos potencialmente afectados.	Actualización completa, evaluación inicial de gravedad e impacto e indicadores de compromiso.	El segundo reporte del OIV se adelanta cuando el incidente afecta la prestación del servicio esencial.	Programa de recuperación, responsables técnicos y administrativos y tiempo estimado de recuperación.	Se envía desde la alerta temprana, siempre que el incidente haya sido gestionado.

DATOS QUE DEBEN ESTAR DISPONIBLES DESDE EL INICIO

Institución y contacto	Cronología	Impacto y alcance	Evidencia técnica
Nombre, RUT, dirección, correo y responsable.	Hora de detección, toma de conocimiento e inicio estimado.	Servicios, activos, usuarios, ubicación y duración.	Indicios, indicadores de compromiso y medidas adoptadas.

Si el incidente no está gestionado al día 15, corresponde remitir un informe parcial y actualizarlo cada 15 días.

ACCIÓN

Plan inicial de 30 días

LEY 21.663

Prioriza acciones que reduzcan la exposición y permitan responder con claridad durante las primeras horas de un incidente.

Semana	Objetivo	Acciones mínimas	Entregable	Responsable
1	**Definir alcance y gobierno**	Confirmar aplicabilidad, revisar calificación OIV, asignar encargado de reportes y establecer escalamiento ejecutivo.	Ficha de alcance + responsables	_____
2	**Identificar lo crítico**	Mapear servicios, procesos, activos, datos y proveedores que sostienen la operación.	Mapa de criticidad y dependencias	_____
3	**Preparar la respuesta**	Documentar clasificación, contactos, reporte ANCI, bitácora y medidas iniciales de contención.	Procedimiento de incidentes	_____
4	**Probar y priorizar**	Ejecutar un ejercicio de mesa, detectar brechas y aprobar un plan de tratamiento con plazos.	Informe de ejercicio + hoja de ruta	_____

REGISTRO DE PRÓXIMAS ACCIONES

Brecha prioritaria	Acción	Responsable	Fecha objetivo	Evidencia de cierre	Estado
_____	_____	_____	___ / ___ / ___	_____	Seleccionar
_____	_____	_____	___ / ___ / ___	_____	Seleccionar

REFERENCIAS

Fuentes oficiales y notas de actualización

LEY 21.663

Esta versión fue elaborada con fuentes oficiales vigentes consultadas en julio de 2026.

Ley N° 21.663, Ley Marco de Ciberseguridad Biblioteca del Congreso Nacional de Chile	Abrir fuente oficial
DecretoSupremo N° 295, Reglamento de reporte de incidentes Biblioteca del Congreso Nacional de Chile	Abrir fuente oficial
Resolución Exenta N °87, primera nómina final de OIV Biblioteca del Congreso Nacional de Chile	Abrir fuente oficial
Instrucción General N° 3, designación del delegado de ciberseguridad Biblioteca del Congreso Nacional de Chile	Abrir fuente oficial
Instrucción General N° 4, medidas para reducir impacto y propagación Biblioteca del Congreso Nacional de Chile	Abrir fuente oficial
Resolución Exenta N° 140, consulta pública de estándares básicos obligatorios Biblioteca del Congreso Nacional de Chile	Abrir fuente oficial

NOTA DE ACTUALIZACIÓN	La ANCI inició el 30 de mayo de 2026 la consulta pública de los estándares básicos obligatorios. Al cierre de esta edición no se identificó una resolución oficial posterior que publicara su versión definitiva.

Recomendación: revisar esta guía cuando la ANCI publique nuevos estándares, instrucciones o nóminas de OIV.

Una preparación útil no termina en el diagnóstico. Debe convertirse en responsables, evidencia y acciones verificables.

I3G Ciberseguridad