

alerta

legal

# NUEVOS OPERADORES DE IMPORTANCIA VITAL:

comienza la etapa de adecuación a la Ley Marco de Ciberseguridad

---

El 24 de julio de 2026 se publicó en el Diario Oficial la Resolución Exenta N° 187 de la Agencia Nacional de Ciberseguridad (“ANCI”) con la nómina definitiva de Operadores de Importancia Vital (“OIV”) correspondiente a la segunda etapa del proceso de calificación establecido por la Ley N° 21.663 Marco de Ciberseguridad.



La nómina incluye entidades de sectores como combustibles, agua potable y saneamiento, transporte, concesiones de servicios públicos, seguridad social, servicios postales y farmacéuticos. También incorpora instituciones de electricidad, telecomunicaciones, salud, infraestructura digital y servicios tecnológicos que no habían sido incluidas en la primera etapa.



Con esta publicación finaliza el procedimiento iniciado en abril, durante el cual la ANCI recibió y analizó 179 observaciones formuladas por las instituciones preliminarmente calificadas, junto con los antecedentes aportados por los organismos públicos con competencia sectorial. Asimismo, comienza el período de adecuación a las obligaciones y estándares especiales aplicables a los OIV.

## 01 INICIO DE LA ETAPA DE ADECUACIÓN

Para las entidades incluidas en la nómina, la prioridad inmediata de una organización calificada como OIV, será generar un programa de adecuación verificable, que articule las áreas de ciberseguridad, tecnologías de la información, continuidad operacional, riesgos, cumplimiento, asuntos legales y gestión de proveedores.

En particular, existen al menos dos hitos regulatorios sujetos a un plazo expreso de 60 días corridos, contado desde la publicación de la nómina definitiva, el cual vence el próximo 22 de septiembre de 2026:

### PLAZO DE ADECUACIÓN

60

días corridos desde la publicación de la nómina definitiva.

### VENCIMIENTO

22/09/2026

Fecha en que vence el plazo de los dos hitos regulatorios.

## 02 DESIGNACIÓN DEL DELEGADO DE CIBERSEGURIDAD

Las entidades calificadas como OIV deberán designar y acreditar ante la ANCI a un delegado de ciberseguridad, de conformidad con la Instrucción General N° 3.

El delegado deberá contar con:



### IDONEIDAD

Formación o experiencia especializada



### INDEPENDENCIA

Independencia funcional suficiente



### REPRESENTACIÓN

Habilitación para representar a la institución ante la ANCI



### REPORTE DIRECTO

Canal de reporte directo a la máxima autoridad o al nivel directivo correspondiente

# 03 PREPARACIÓN PARA CONTENER Y MITIGAR INCIDENTES

La Instrucción General N° 4 exige que los OIV cuenten con procedimientos y capacidades que permitan adoptar medidas inmediatas para reducir el impacto y evitar la propagación de incidentes de ciberseguridad.

Entre otras materias, las instituciones deberán revisar sus capacidades para:

01 Aislar sistemas y segmentos de red afectados.

02 Restringir accesos administrativos y remotos.

03 Gestionar cuentas privilegiadas y eliminar cuentas no utilizadas.

04 Proteger y separar los sistemas de respaldo.

05 Mantener mecanismos adecuados de segmentación de redes y cortafuegos.

06 Registrar las decisiones y medidas adoptadas durante un incidente.

07 Preservar evidencia e informar oportunamente al nivel directivo y a la ANCI.

## 04 ¿CÓMO ABORDAR LA ADECUACIÓN?

Como primera medida, las entidades calificadas como OIV deberían identificar los servicios, procesos, instalaciones, activos y dependencias tecnológicas que fundamentaron su inclusión en la nómina. La propia resolución entrega antecedentes sectoriales relevantes sobre los factores considerados por la ANCI, tales como la dependencia tecnológica, la falta de proveedores alternativos, la interdependencia con otros servicios esenciales y el impacto potencial de una interrupción.

Sobre esa base, será recomendable desarrollar un diagnóstico que permita:



Contrastar las políticas, procedimientos y controles existentes con las obligaciones aplicables a los OIV.



Identificar brechas de gobernanza, continuidad operacional, gestión de incidentes, seguridad de redes y administración de terceros.



Definir responsables, prioridades, recursos y plazos mediante un plan de adecuación aprobado por la alta administración.



Mantener evidencia suficiente de las decisiones, controles, ejercicios, capacitaciones y medidas implementadas.

El objetivo de la adecuación será integrar las nuevas exigencias en la gestión ordinaria de riesgos, continuidad operacional, seguridad de la información y supervisión de proveedores.

## 05 POSIBILIDAD DE IMPUGNAR LA CALIFICACIÓN

Las entidades que estimen que no concurren los requisitos para su calificación como OIV podrán evaluar los recursos administrativos contemplados en la Ley N° 19.880 y la reclamación judicial prevista en la Ley Marco de Ciberseguridad.



Considerando los plazos regulatorios que empiezan a correr desde la publicación, la evaluación de una eventual impugnación debería desarrollarse paralelamente a la identificación de brechas y a la preparación de las medidas de cumplimiento más inmediatas.

### ETAPA PRÁCTICA

La publicación de la nómina definitiva marca así el comienzo de una etapa práctica, en la que las entidades calificadas como OIV deberán demostrar que cuentan con estructuras de gobernanza, procedimientos y capacidades técnicas efectivamente implementadas para prevenir, gestionar y responder a incidentes de ciberseguridad.

El presente boletín fue creado en español y no constituye asesoría legal. Guerrero Olivos no será responsable por actos u omisiones de terceros basados en la información contenida en él.

## contacto



**Rocío García  
de la Pastora**

[rgarciadelapastora@guerrero.cl](mailto:rgarciadelapastora@guerrero.cl)



**Tomás  
Garnham**

[tgarnham@guerrero.cl](mailto:tgarnham@guerrero.cl)



**Diego  
Morandé**

[dmorande@guerrero.cl](mailto:dmorande@guerrero.cl)



**Pedro  
Pellegrini**

[ppellegrini@guerrero.cl](mailto:ppellegrini@guerrero.cl)



**Alejandra  
Leiton**

[aleiton@guerrero.cl](mailto:aleiton@guerrero.cl)



**Joaquín  
Valenzuela**

[jvalenzuelac@guerrero.cl](mailto:jvalenzuelac@guerrero.cl)



**Paulina  
Ferreras**

[pferreras@guerrero.cl](mailto:pferreras@guerrero.cl)



**Vicente  
Sapag**

[vsapag@guerrero.cl](mailto:vsapag@guerrero.cl)



**Felipe  
Spoerer**

Procurador