ALERTA LEGAL

Entrada en vigencia obligación de reportar incidentes de ciberseguridad

4.03.2025

Cariola Díez Pérez-Cotapos

Entrada en vigencia obligación de reportar incidentes de ciberseguridad

El sábado 01 de marzo entró en vigor la obligación de reportar ciberataques o incidentes de ciberseguridad, bajo la **Ley N° 21.663 marco de ciberseguridad (LMC)**. Asimismo, ese día se publicaron en el Diario Oficial la **Resolución 295/2024** que aprueba el reglamento de reporte de incidentes de ciberseguridad y la **Resolución Ex. 7/2025** que fija la taxonomía de los incidentes.

Entidades Obligadas: Instituciones calificadas como prestadores de servicios esenciales (PSE) u operadores de importancia vital (OIV). La Agencia Nacional de Ciberseguridad (ANCI) aún no define las instituciones que serán consideradas OIV.

Incidentes que deben reportarse: Cualquier **ciberataque o incidente de ciberseguridad con efectos significativos.**

Se considera que un incidente de ciberseguridad tiene **efecto significativo** si es capaz de producir **alguno de los siguientes efectos:**

- Interrumpir la continuidad de un servicio esencial. Debe considerarse, tanto los servicios entregados por proveedores, como la cadena de suministro, de una institución que preste servicios esenciales o de un operador de importancia vital.
- Afectar la integridad física o la salud de las personas.
- Afectar la integridad o confidencialidad de activos informáticos, o la disponibilidad de alguna red o sistema informático, aun cuando esto no produzca o hubiere producido afectación inmediata en la provisión del servicio.
- Utilizar o ingresar sin autorización a redes o sistemas informáticos, aun cuando esto no produzca o hubiere producido afectación inmediata en la provisión del servicio.
- Afectar sistemas informáticos que contengan datos personales.

A quién se reporta: El reporte de ciberataque o incidente de ciberseguridad con efectos significativos debe enviarse al Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional) mediante los siguientes canales:

- **Vía plataforma de reporte:** https://portal.anci.gob.cl para lo cual se **requiere ClaveÚnica** de la persona que reporta.
- **Canales alternativos:** La ANCI ha informado que adicionalmente, se mantendrán operativos los siguientes canales disponibles para reportar y comunicarse con la ANCI **en caso de contingencias:** teléfono 1510, correo electrónico ayuda@anci.gob.cl

Contenido del reporte: El reporte debe contener la información indicada en la Resolución 295, incluyendo la institución afectada, datos de contacto del delegado de ciberseguridad, información sobre el incidente (fecha, hora, indicios de la ocurrencia, activos y recursos potencialmente afectados, indicadores de compromiso), si la acción se encuentra tipificada como delito, repercusiones a otras instituciones y cualquier otro dato que sea útil para la gestión del incidente.

La descripción del incidente debe considerar la **taxonomía de incidentes indicada en la Resolución Ex. 7/2025** que contempla cuatro áreas de impacto y once efectos observables.

Plazo para reportar: Una vez que la institución hubiere tomado conocimiento de la ocurrencia de un incidente de ciberseguridad, deberá enviar una alerta sobre la ocurrencia del mismo en el **plazo máximo de 3 horas desde que se toma conocimiento** del incidente. Luego, transcurrido el plazo máximo de **72 horas**, deberá enviar un **segundo reporte** al CSIRT Nacional y dentro del

plazo máximo de **15 días corridos** contados desde el envío de la alerta temprana, la institución deberá elaborar un informe final.

Sanciones: La omisión de reportar los ciberataques o incidentes de ciberseguridad es una infracción grave bajo la LMC, que se sanciona con una multa de hasta 10.000 UTM equivalente a USD 715.396 aproximadamente. Una vez se definan las entidades calificadas como OIV, éstas podrán ser sancionadas con una multa de hasta 20.000 UTM, equivalente a USD1.415.277 aproximadamente.

Relación obligación de reportes a nivel sectorial

En caso de que el sujeto obligado de LMC tenga la obligación de reportar incidentes en base a la regulación sectorial que le fuera aplicable (por ejemplo, en materia bancaria y financiera o de telecomunicaciones), deberá adicionalmente seguir cumpliendo con tal obligación en los plazos y formas que la normativa sectorial establezca.

Recomendaciones:

- Designar a una persona responsable de reportar incidentes que tenga ClaveÚnica, debidamente capacitado sobre las obligaciones de la LMC.

- Generar un protocolo de actuación ante la ocurrencia de ciberataques o incidentes de ciberseguridad con efectos significativos, que contemple:

  a) Mecanismos de detección y respuesta inmediata, estableciendo procedimientos para la identificación temprana de amenazas y la activación de medidas de contención que prevengan su propagación;

  b) Proceso de notificación obligatoria al CSIRT Nacional y al regulador sectorial si existiese obligación de reporte, asegurando el cumplimiento del o los plazos de reporte;

  c) Clasificación del incidente, según la taxonomía definida por la ANCI, y el regulador sectorial si existiese obligación, considerando sus impactos en confidencialidad, integridad y disponibilidad;

  d) Plan de mitigación y recuperación, que contemple acciones inmediatas para la contención del incidente, la restauración de servicios esenciales y la continuidad operacional;

  e) Registro detallado del incidente y medidas adoptadas; y

  f) Capacitación y simulacros periódicos, dirigidos a fortalecer la resiliencia organizacional y optimizar la respuesta ante futuros incidentes.

Contactos:

Carolina Filsfisch
Socia

Gabriel Pensa
Asociado Senior

Eduardo Vilches
Asociado Senior