DIARIO OFICIAL
DE LA REPUBLICA DE CHILE
Ministerio del Interior

I SECCIÓN

LEYES, REGLAMENTOS, DECRETOS Y RESOLUCIONES DE ORDEN GENERAL

Núm. 44.333-B | Viernes 26 de Diciembre de 2025 | Página 1 de 4

Normas Generales

CVE 2747332

MINISTERIO DE SEGURIDAD PÚBLICA

Agencia Nacional de Ciberseguridad

INSTRUCCIÓN GENERAL N° 4

IMPARTE INSTRUCCIONES SOBRE LAS MEDIDAS NECESARIAS PARA REDUCIR EL IMPACTO Y LA PROPAGACIÓN DE UN INCIDENTE DE CIBERSEGURIDAD, CONFORME AL ARTÍCULO 8 LITERAL E) DE LA LEY N° 21.663

A: INSTITUCIONES CALIFICADAS COMO OPERADORES DE IMPORTANCIA VITAL SEGÚN LO ESTABLECIDO EN EL ARTÍCULO 6° DE LA LEY N° 21.663.
FECHA: 22 DE DICIEMBRE DE 2025

Visto:

Lo dispuesto en la ley N° 21.663, Marco de Ciberseguridad;

Considerando:

1. Que, todas las instituciones públicas y privadas calificadas como operadores de importancia vital de conformidad con lo dispuesto en el artículo 6° de la ley N° 21.663, marco de ciberseguridad (“la ley”), deben cumplir un conjunto de deberes específicos de ciberseguridad establecidos en el artículo 8° de la ley;

2. Que, el literal e) del artículo 8° de la ley establece que los Operadores de Importancia Vital deberán adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad, incluida la restricción de uso o el acceso a sistemas informáticos, si fuera necesario;

3. Que, conforme a lo dispuesto en el literal b) del artículo 11° de la ley, para dar cumplimiento a su objeto, la Agencia Nacional de Ciberseguridad (en adelante, indistintamente “la Agencia” o “ANCI”) tiene la atribución de dictar instrucciones generales y particulares, de carácter obligatorio, para las instituciones, tanto públicas como privadas obligadas por dicha ley, y las demás disposiciones necesarias para la aplicación y el cumplimiento de esta y sus reglamentos.

4. Que, en mérito de lo anteriormente indicado, se dicta la siguiente instrucción de carácter general:

Artículo primero. Restricción de uso y aislamiento de sistemas afectados.

Ante la ocurrencia de un incidente de ciberseguridad, los Operadores de Importancia Vital deberán adoptar, de forma inmediata, las medidas necesarias para:

a) Restringir total o parcialmente el acceso a los sistemas informáticos, redes, servicios o cuentas de usuario que se encuentren comprometidos o respecto de los cuales exista riesgo de compromiso;

b) Aislar los sistemas afectados del resto de la infraestructura tecnológica, cuando ello resulte necesario para evitar la propagación del incidente;

c) Suspender temporalmente funcionalidades, integraciones o accesos remotos que puedan facilitar la expansión del incidente.

Estas medidas podrán implicar la interrupción temporal o parcial de servicios, cuando ello sea necesario para proteger otros activos críticos o servicios esenciales.

Artículo segundo. Cambio de contraseñas de usuarios con acceso administrativo a los sistemas afectados y eliminación de cuentas no utilizadas.

Detectado un incidente de ciberseguridad con impacto en la confidencialidad de la información, en la integridad de la información, o en el uso legítimo de recursos, categorías descritas en la taxonomía de incidentes publicada en la resolución N° 7 de 2025, de la Agencia, la institución deberá adoptar las medidas necesarias para cambiar inmediatamente las contraseñas de todas las cuentas de usuario con permisos totales o parciales de administración de redes, sistemas e infraestructura en los sistemas afectados, o sobre los cuales existe sospecha de afectación.

Asimismo, la institución deberá revisar todos los sistemas anteriormente mencionados y eliminar inmediatamente aquellas cuentas administrativas que sean genéricas o no estén asociadas a funcionarios o proveedores activos, creando previamente, si no existiese, al menos una cuenta administrativa personal.

Estas medidas deberán ser adoptadas dentro de las primeras tres horas de tomado conocimiento del incidente, informando a la Agencia Nacional de Ciberseguridad en la alerta temprana del proceso de reporte de incidentes, el listado de cuentas modificadas o eliminadas.

Con todo, las medidas señaladas en el inciso segundo anterior deberán ser adoptadas de manera preventiva por las instituciones, al menos, cada seis meses.

Artículo tercero. Deshabilitación de accesos remotos o administrativos expuestos.

Detectado un incidente de ciberseguridad, los operadores de importancia vital deberán:

a) Revisar que no existan accesos remotos o administrativos expuestos públicamente a Internet. En caso de detectar su existencia, deberán ser informados a la Agencia en la alerta temprana del proceso de reporte de incidentes, además de ser bloqueados o dados de baja dentro de las primeras tres horas de toma de conocimiento del incidente;

b) Permitir el acceso exclusivamente a través de la VPN institucional, en caso de existir sistemas de acceso remoto expuestos a Internet. En la eventualidad de que la infraestructura de VPN no pudiese ser utilizada, el acceso debe restringirse solamente a conexiones desde segmentos o direcciones IP específicas indispensables, para la gestión del incidente, bloqueando y llevando registro de cualquier intento de conexión desde un origen no permitido explícitamente;

c) Configurar mecanismos seguros de acceso remoto, con credenciales aleatorias y, en caso de ser factible su configuración inmediata, el uso obligatorio de autenticación multifactor;

d) Deshabilitar todo acceso remoto tan pronto como la tarea que le dio origen durante el proceso de gestión del incidente se haya completado.

Artículo cuarto. Protección de comunicaciones y suspensión de servicios expuestos.

Cuando un incidente de ciberseguridad afecte, o pueda afectar, servicios expuestos a Internet, los operadores de importancia vital deberán:

a) Suspender temporalmente la operación de sitios web, servicios transaccionales o interfaces expuestas, cuando exista riesgo de explotación activa, añadiendo un mensaje que informe de su suspensión intencional como medida mitigatoria de seguridad;

b) Redireccionar o limitar el acceso a dichos servicios únicamente a entornos confidenciales e íntegros, cuando ello sea técnicamente viable;

c) Asegurar que, en caso de mantenerse operativos, dichos servicios utilicen mecanismos de cifrado robustos y correctamente configurados, con el objeto de evitar la interceptación o manipulación de las comunicaciones durante el incidente.

Artículo quinto. Uso de herramientas de seguridad para detección y contención.

Los operadores de importancia vital deberán contar con herramientas de seguridad que les permitan realizar las siguientes acciones durante la gestión de un incidente de ciberseguridad:

a) Identificar dispositivos, cuentas o procesos comprometidos;

b) Bloquear, aislar o deshabilitar de forma remota dichos dispositivos o cuentas;

c) Monitorear la evolución del incidente y detectar intentos de propagación a otros sistemas.

Las herramientas señaladas en el presente artículo podrán corresponder tanto a soluciones comerciales como a herramientas gratuitas o de código abierto, siempre que permitan cumplir de manera efectiva con las acciones de detección, contención y monitoreo del incidente descritas precedentemente.

Con el objeto de apoyar a las instituciones en la adopción de estas medidas, la Agencia Nacional de Ciberseguridad podrá publicar y mantener actualizada una referencia no exhaustiva de herramientas de seguridad que hayan sido evaluadas como confiables para estos fines, la cual tendrá carácter orientador y no eximirá a las instituciones de su responsabilidad en la adecuada selección, configuración y uso de dichas herramientas.

Artículo sexto. Uso de cortafuegos.

Los Operadores de Importancia Vital deberán instalar y mantener en operación cortafuegos (firewalls) adecuados a la naturaleza, complejidad y nivel de riesgo de sus sistemas informáticos. En cualquier caso, las políticas de seguridad deberán ser configuradas bajo el principio de bloqueo de conexiones entrantes por defecto (whitelisting).

Será responsabilidad de la institución establecer los lineamientos, directrices y requisitos mínimos de seguridad que deberán observarse en la configuración y uso de los cortafuegos, así como supervisar y verificar de manera periódica que dichos lineamientos sean implementados.

Artículo séptimo. Segmentación de redes y contención de propagación lateral.

Con el objeto de reducir el impacto y evitar la propagación de un incidente de ciberseguridad, los Operadores de Importancia Vital deberán adoptar medidas de segmentación lógica y/o física de redes que permitan limitar el movimiento lateral del incidente entre sistemas, entornos y activos críticos.

En particular, una vez detectado un incidente de ciberseguridad, o ante la sospecha de su ocurrencia, la institución deberá:

a) Aislar de forma inmediata los segmentos de red, entornos de virtualización, servidores físicos o lógicos, y otros activos digitales respecto de los cuales exista compromiso o riesgo razonable de compromiso;

b) Restringir o bloquear el tráfico de red entrante y saliente entre sistemas productivos, entornos de respaldo, sistemas de gestión, administración o monitoreo, excepto cuando dicha comunicación sea estrictamente necesaria para la contención del incidente;

c) Implementar, cuando sea técnicamente posible, segmentación específica para entornos de virtualización;

d) Separar y proteger los sistemas de respaldo del resto de la infraestructura afectada, restringiendo su acceso y comunicación durante la gestión del incidente;

e) Suspender temporalmente las credenciales, integraciones o servicios compartidos que permitan el desplazamiento lateral del incidente entre segmentos de red.

Las medidas de segmentación y aislamiento deberán mantenerse vigentes mientras persista el riesgo de propagación del incidente, y su levantamiento deberá realizarse de manera gradual y controlada, una vez mitigado dicho riesgo.

La institución deberá asegurar que las decisiones adoptadas queden debidamente registradas, incluyendo su alcance, duración y justificación.

Artículo octavo. Coordinación interna y registro de medidas adoptadas.

La institución deberá coordinar la adopción de las medidas señaladas en la presente instrucción y asegurar que:

a) Las decisiones adoptadas durante la gestión del incidente queden debidamente registradas;

b) Toda la evidencia que se recolecte durante el incidente sea guardada de manera confidencial y protegida, para ser revisada posteriormente;

c) Se mantenga en comunicación con personal de la Agencia de manera continua durante el incidente para coordinar la respuesta al mismo;

d) Se mantenga informado al nivel directivo correspondiente de la institución, sobre las medidas de restricción, aislamiento o suspensión de servicios adoptadas y sus eventuales impactos operacionales.

Artículo noveno. Vigencia.

Las instituciones obligadas dispondrán de un plazo de sesenta días corridos, contado desde la publicación en el Diario Oficial de la nómina final de calificación de operadores de importancia vital mediante la cual hayan sido calificadas como tales, para dar cumplimiento a las obligaciones establecidas en esta instrucción.

Anótese y publíquese.- Daniel Álvarez Valenzuela, Director Nacional, Agencia Nacional de Ciberseguridad.