CIRCULAR N°

Correlativo Interno N° [O-78193-2026]

[IMPARTE INSTRUCCIONES A LAS ENTIDADES QUE INDICA SOBRE LAS ACCIONES DE CIBERSEGURIDAD QUE DEBEN ADOPTAR CONFORME A LA LEY N°21.663.

MODIFICA EL COMPENDIO NORMATIVO SOBRE LICENCIAS MÉDICAS, SUBSIDIOS POR INCAPACIDAD LABORAL Y SEGURO SANNA, COMPENDIO DE NORMAS QUE REGULAN A LAS CAJAS DE COMPENSACIÓN DE ASIGNACIÓN FAMILIAR Y COMPENDIO DE NORMAS QUE REGULAN A LOS SERVICIOS DE BIENESTAR DEL SECTOR PÚBLICO]

Esta Superintendencia, en su rol de entidad encargada de supervigilar y fiscalizar los regímenes de seguridad social, de protección social y las instituciones que los administren, conforme lo dispone la Ley N° 16.395, en cumplimiento de su obligación de impartir instrucciones a las instituciones sometidas a su fiscalización sobre los procedimientos para el adecuado otorgamiento de las prestaciones y, además, en su calidad de entidad autoridad sectorial, conforme a los artículos 25 y 26 de la Ley N°21.663, ha estimado necesario emitir las instrucciones necesarias para fortalecer la ciberseguridad en las instituciones dedicadas a la administración de prestaciones de seguridad social, mediante la modificación del Compendio de Normas sobre Licencias Médicas, Subsidios de Incapacidad Laboral y Seguro SANNA, Compendio de Normas que regulan a las Cajas de Compensación de Asignación Familiar y el Compendio de Normas que regulan a los Servicios de Bienestar del Sector Público, previa coordinación con la Agencia Nacional de Ciberseguridad (ANCI).

La Ley N°21.663, que entró en vigencia el 1 de enero y el 1 de marzo de 2025, en virtud de lo dispuesto en el artículo 2° del DFL 1-21.663, de 2024, del Ministerio del Interior y Seguridad Pública, establece en su artículo 4° que se aplicará a las instituciones que presten servicios calificados como esenciales (PSE) y aquellas calificadas como operadores de importancia vital (OIV).

Al respecto, la referida Ley precisa por un lado que, son servicios esenciales, los provistos por Organismos de la Administración del Estado, como por ejemplo, las Comisiones de Medicina Preventiva e Invalidez (COMPIN) y los Organismos a que pertenecen los Servicios de Bienestar que fiscaliza esta Superintendencia y, por otro lado, también prestan servicios esenciales las instituciones privadas que realizan actividades de administración de prestaciones de seguridad social, como por ejemplo, los Operadores del sistema de información que permite el otorgamiento y tramitación electrónica de las licencias médicas (Operadores LME), las Instituciones de Salud Previsional (Isapre) y las Cajas de Compensación de Asignación Familiar (C.C.A.F.). Finalmente, el citado cuerpo legal especifica que los OIV son las entidades calificadas como tal por la ANCI, en virtud del procedimiento descrito en los artículos 5° y 6° de la referida Ley.

En este contexto, la ANCI dictó la Resolución N° 187 exenta, de 2026, calificando a los Operadores LME, Isapre y las C.C.A.F. como OIV. Tal calificación implica que la provisión de sus servicios depende de redes y sistemas informáticos cuya afectación, interceptación, interrupción o destrucción tendría un impacto significativo en la seguridad y el orden público, en la provisión continua y regular de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado o de los servicios que debe proveer o garantizar. En consecuencia, atendida su relevancia, la Ley le exige a estas entidades cumplir diversas obligaciones críticas, como por ejemplo implementar un sistema de gestión de seguridad de información continuo, informar en breve plazo el plan de acción ante incidentes de ciberseguridad que puedan tener efectos significativos, entre otras, cuya infracción conlleva la aplicación de multas de hasta 40.000 UTM.

En consecuencia, por las consideraciones expuestas corresponde impartir instrucciones en los términos que a continuación se indican.

I. MODIFÍCASE EL COMPENDIO DE NORMAS SOBRE LICENCIAS MÉDICAS, SUBSIDIOS DE INCAPACIDAD LABORAL Y SEGURO SANNA, DE LA SIGUIENTE MANERA:

1. **SUPRÍMASE** el numeral 7, del Título IV, del Libro VI, pasando el numeral 8 a ser el 7.

2. CRÉASE el "LIBRO VIII. Aspectos operacionales y administrativos" e **INCORPÓRASE** en él el siguiente Título I:

"**TÍTULO I: ACCIONES DE CIBERSEGURIDAD**

1. ASPECTOS GENERALES

Con la finalidad de proteger a las personas, la sociedad, las organizaciones y la nación ante incidentes de ciberseguridad, las instituciones que prestan servicios calificados como esenciales (PSE), conforme al artículo 4° de la Ley N°21.663, y aquellas que sean calificadas como operadores de importancia vital (OIV) por Resolución de la Agencia Nacional de Ciberseguridad (ANCI), deben cumplir las obligaciones de la referida Ley y los protocolos, estándares técnicos o instrucciones de carácter general que emita sobre la materia la ANCI y las instrucciones que emita la autoridad sectorial respectiva.

Las Instituciones de Salud Previsional (Isapres), las Cajas de Compensación de Asignación Familiar (C.C.A.F.) y los Operadores del sistema de información que permite el otorgamiento y tramitación electrónica de las licencias médicas (Operadores LME) revisten la calidad de PSE y fueron calificados como OIV mediante la Resolución Exenta N°187 de 2026 de la ANCI. En consecuencia, las Isapres y Operadores LME deberán cumplir las instrucciones contenidas en este Título, mientras que las C.C.A.F. deberán ceñirse a lo dispuesto en el numeral 6.1.12 del Compendio de Normas que Regulan a las Cajas de Compensación de Asignación Familiar.

Por su parte, las Comisiones de Medicina Preventiva e Invalidez (COMPIN), en su condición de Organismos de la Administración del Estado dependientes de las SEREMI de Salud, deberán cumplir estrictamente las obligaciones de ciberseguridad fijadas en la ley, los protocolos e instrucciones generales de la ANCI y las normas que dicte la autoridad sectorial respectiva.

2. PREVENCIÓN Y GESTIÓN DE RIESGO DE CIBERSEGURIDAD

2.1. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) CONTINUO

Los Operadores LME y las Isapre, en tanto PSE, deben cumplir el deber general de aplicar de manera permanente medidas tecnológicas, organizacionales, físicas y/o informativas para prevenir, reportar y resolver incidentes de ciberseguridad. Para el cumplimiento de estas obligaciones deben implementar los protocolos y estándares que establecerá la ANCI y estándares que establezca la Superintendencia de Seguridad Social.

Sin perjuicio de lo anterior, considerando que dichas entidades fueron calificadas como OIV les corresponde aplicar dichas medidas a través de la implementación

de un Sistema de Gestión de Seguridad de la Información (SGSI) continuo para determinar aquellos riesgos que puedan afectar la seguridad de las redes, sistemas informáticos y datos, y la continuidad operacional del otorgamiento y tramitación electrónica de las licencias médicas y la gestión y pago del subsidio por incapacidad laboral. Dicho sistema, además, deberá permitir evaluar, tanto la probabilidad como el potencial impacto de un incidente de ciberseguridad. Asimismo, las referidas entidades deberán mantener un registro de las acciones ejecutadas que compongan el SGSI, de conformidad a lo que señale el reglamento respectivo.

Los Operadores LME y las Isapre, deben elaborar e implementar planes de continuidad operacional y ciberseguridad que sean debidamente certificados, en conformidad al artículo 28 de la Ley N°21.663 y sometidos a revisiones periódicas, con una frecuencia mínima de dos años. Asimismo, continuamente realizarán operaciones de revisión, ejercicios, simulacros y análisis de las redes, sistemas informáticos y sistemas para detectar acciones o programas informáticos que comprometan la ciberseguridad y comunicar la información relativa a dichas acciones o programas al CSIRT Nacional, en la forma que determine el reglamento respectivo.

De conformidad con la Instrucción General N°4, de 2025, de la ANCI las referidas entidades 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 y, además, deberá contar con las certificaciones que señala el artículo 28 de la Ley N°21.663.

Por otro lado, deberá entregar información veraz, suficiente y oportuna a los potenciales afectados, en la medida que puedan identificarse y cuando así lo requiera la ANCI, sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente su información o redes y sistemas informáticos, especialmente cuando involucran datos personales y no exista otra disposición legal que requiera su notificación; o cuando sea necesario para prevenir la ocurrencia de nuevos incidentes o para gestionar uno que ya hubiera ocurrido.

Finalmente, deberán designar a uno o más delegados de ciberseguridad y encargados de reportar, conforme a los numerales 2.2. y 2.3. siguientes, y contar con programas de capacitación, formación y educación continua de sus trabajadores y colaboradores, que incluyan campañas de ciberhigiene.

La Política de Seguridad de la Información que elaboren e implementen los Operadores LME e Isapres, en el marco de la certificación del SGSI, deberá ser reportada a la Superintendencia de Seguridad Social, para su conocimiento, a través del Sistema GRIS-LM , conforme al numeral 3, del Título VI, del Libro VII, de este Compendio.

2.2. DELEGADO DE CIBERSEGURIDAD

Los Operadores LME e Isapres, designarán al menos a un delegado de ciberseguridad, quien deberá tener formación, certificación o experiencia especializada, en el nivel técnico o profesional, en materia de ciberseguridad, gestión de riesgos tecnológicos, continuidad operacional o disciplinas afines. Para estos efectos, deberán realizar la designación de conformidad con las instrucciones contenidas en la Instrucción General N°3, de 2025, de la ANCI.

El delegado de ciberseguridad desempeñará las siguientes funciones:

a. Actuará como contraparte de la ANCI, pudiendo solicitarle asesoría técnica ante la ocurrencia de incidentes de ciberseguridad que hayan comprometido sus activos informáticos críticos o afectado el funcionamiento de su operación. Además, informará a la máxima autoridad institucional señalada en el literal i) del artículo 8° de la ley.
b. Podrá asesorar a la institución en la elaboración de los programas de capacitación, formación y educación continua de los trabajadores y colaboradores, incluyendo campañas de ciberhigiene.
c. Capacitará al personal de la entidad en temáticas sobre prevención de incidentes de ciberseguridad y acciones ante ciberataques, al menos cada seis meses.
d. Podrá asesorar a la institución en el procedimiento para obtener las certificaciones de ciberseguridad que señala la Ley N°21.663 y las que determine la ANCI.
e. Incluirá en los planes de continuidad operacional y ciberseguridad las mantenciones planificadas que produzcan o pudieren producir indisponibilidad de los sistemas informáticos de la institución.

Para que el delegado de ciberseguridad desempeñe adecuadamente sus funciones, los Operadores LME y las Isapres, deberán habilitarle un canal de comunicación y reporte directo a la máxima autoridad institucional, otorgarle independencia funcional suficiente para comunicar riesgos, incidentes y brechas de cumplimiento a la autoridad interna, sin interferencias de áreas operativas de la institución que pudiesen comprometer la objetividad de dichas comunicaciones y habilitarlo para representar a la institución ante la ANCI.

Los Operadores LME y las Isapres deberán informar a la Superintendencia de Seguridad Social, a través del Sistema GRIS-LM, conforme al numeral 3, del Título VI, del Libro VII, de este Compendio, sobre la designación del delegado de ciberseguridad y sus subrogantes y cualquier modificación que efectúe a dicha designación.

2.3. ENCARGADO DE REPORTAR

Los Operadores LME y las Isapres designarán a una o más personas encargadas de reportar los ciberataques e incidentes de ciberseguridad, definidos en el artículo 2° de la referida Ley, al Equipo de Respuesta a Incidentes de Seguridad

Informática (CSIRT) Nacional que puedan tener efectos significativos en los términos del artículo 27 de la Ley N°21.663.

La o las personas encargadas de reportar deberán tener formación o experiencia técnica o profesional en ciberseguridad, serán designados conforme a las Instrucciones Generales N°s 1 y 2, de 2025, de la ANCI y desempeñará, al menos, las siguientes funciones:

a. Mantener una relación fluida con el CSIRT Nacional a través de la plataforma de la ANCI y los otros medios de contacto que esa entidad disponga.
b. Inscribir a la institución en la plataforma de la ANCI, siguiendo las Instrucciones Generales N°s 1 y 2, de 2025, de la ANCI, y estará obligado a mantener la confidencialidad de sus credenciales, siendo responsable por su uso indebido, o por su utilización por parte de terceras personas.
c. Podrá colaborar en las funciones del delegado de ciberseguridad.

El encargado de reportar puede ser, además, delegado de ciberseguridad, siempre que cumpla con el perfil exigido para ello en el literal 2.2.

Los Operadores LME y las Isapres deberán informar a la Superintendencia de Seguridad Social, a través del Sistema GRIS-LM, conforme al numeral 3, del Título VI, del Libro VII, de este Compendio, sobre la designación del encargado de reportar y sus subrogantes y cualquier modificación que efectúe a dicha designación.

3. CONTENCIÓN Y MITIGACIÓN DE INCIDENTES DE CIBERSEGURIDAD

A) REPORTE DE CIBERATAQUES E INCIDENTES DE CIBERSEGURIDAD

Los Operadores LME y las Isapres, deben reportar oportunamente a la Superintendencia de Seguridad Social la ocurrencia de un ciberataque o un incidente de ciberseguridad, que no puedan tener efectos significativos, a través del Sistema GRIS LM, conforme al numeral 3, del Título VI, del Libro VII, de este Compendio.

Sin embargo, cuando el ciberataque o incidente de ciberseguridad pudiera tener efectos significativos, conforme lo dispone el artículo 27 de la Ley N°21.663, el encargado de reportar, deberá enviar, a través de la ventanilla única, los reportes a que se refiere el artículo 9 de la referida Ley y las actualizaciones sobre la situación que se le requieran, en base a la taxonomía establecida en la Resolución N° 7 exenta, de 2025, de la ANCI. Además, deberán informar al CSIRT Nacional su plan de acción, tan pronto lo hubieren adoptado.

Los Operadores LME y las Isapres deberán omitir en los reportes y actualizaciones, todo dato o información personal, conforme a la Ley N°19.628. Para estos efectos, la dirección IP no se considerará dato o información personal.

B) ENVÍO DE INFORMACIÓN REQUERIDA POR LA ANCI Y EL CSIRT NACIONAL

Con la finalidad de prevenir la ocurrencia de incidentes de ciberseguridad o gestionar uno que ya hubiera ocurrido, la ANCI, de manera particular, específica y fundada, podrá requerir a los Operadores LME y las Isapre, que le otorguen acceso a la información estrictamente necesaria para ello, o bien, la entrega del registro de actividades de las redes y sistemas informáticos que permitan comprender detalladamente los incidentes de ciberseguridad que puedan haber ocurrido. La referida información deberá ser remitida en el más breve plazo, con los datos personales debidamente anonimizados, si fuera posible sin entorpecer la gestión de incidentes y efectuando su tratamiento en estricto cumplimiento de la Ley N°19.628, teniendo presente que la dirección IP no es un dato personal. De todas maneras, podrá entregar la información requerida en calidad de reservada, en virtud del artículo 35 de la Ley N°21.663.

En caso de incidentes de impacto cuya gestión lo haga imprescindible, la ANCI podrá requerir, mediante instrucción del Director o Directora, el acceso a redes y sistemas informáticos de los Operadores LME E Isapres, pero cuando requiera restringir el acceso o uso de redes o sistemas informáticos utilizados para el otorgamiento y tramitación de licencias médicas, deberá actuar conjuntamente con la Superintendencia de Seguridad Social. Ante estos requerimientos, la entidad podrá oponerse o proporcionar todas las facilidades de acceso que sean necesarias, conforme lo dispone la letra k) de la Ley N°21.663.

El mismo procedimiento se aplicará cuando la ANCI requiera el acceso a sistemas informáticos, datos, documentos y demás información que fuere necesaria para el desempeño de sus funciones de supervisión y fiscalización.

Por otro lado, los Operadores LME e Isapres deberán remitir al CSIRT Nacional, cuando lo requiera, la información anonimizada de incidentes de ciberseguridad, las vulnerabilidades encontradas y los planes de acción respectivos para mitigarlos.

Los Operadores LME y las Isapres deberán informar a la Superintendencia de Seguridad Social, a través del Sistema GRIS-LM, conforme al numeral 3, del Título VI, del Libro VII, de este Compendio, los requerimiento de información que le efectúe la ANCI o el CSIRT."

II. MODIFÍCASE EL NUMERAL 6.1., DEL COMPENDIO DE NORMAS QUE REGULAN A LAS CAJAS DE COMPENSACIÓN DE ASIGNACIÓN FAMILIAR, DE LA SIGUIENTE FORMA:

1. **REEMPLÁZASE** el numeral 6.1.12 por el siguiente:

"6.1.12 ACCIONES DE CIBERSEGURIDAD

6.1.12.1. ASPECTOS GENERALES

Con la finalidad de proteger a las personas, la sociedad, las organizaciones y la nación ante incidentes de ciberseguridad, las instituciones que prestan servicios calificados como esenciales (PSE) y aquellas que sean calificadas como operadores de importancia vital (OIV), deben cumplir las obligaciones establecidas en la Ley N°21.663 y los protocolos, estándares técnicos o instrucciones de carácter general que emita sobre la materia la Agencia Nacional de Ciberseguridad (ANCI) y la Superintendencia de Seguridad Social, conforme a los artículos 25 y 26 de la referida Ley.

La Cajas de Compensación de Asignación Familiar son entidades privadas que administran prestaciones de seguridad social y, en virtud de los artículos 4° y 5° de la Ley N°21.663 y la Resolución N° 187 exenta, de 2026, de la ANCI son PSE calificadas como OIV, por consiguiente, les corresponde cumplir, tanto las obligaciones generales como los deberes específicos que el citado cuerpo legal le encomienda y las instrucciones contenidas en este numeral.

6.1.12.2. MODELO DE PREVENCIÓN Y GESTIÓN DE RIESGO DE CIBERSEGURIDAD

6.1.12.2.1. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) CONTINUO

Las Cajas de Compensación de Asignación Familiar, en tanto PSE, deben cumplir el deber general de aplicar de manera permanente medidas tecnológicas, organizacionales, físicas y/o informativas para prevenir, reportar y resolver incidentes de ciberseguridad. Para el cumplimiento de estas obligaciones deben implementar los protocolos y estándares que establecerá la ANCI y estándares que establezca la Superintendencia de Seguridad Social.

Sin perjuicio de lo anterior, considerando que dichas entidades fueron calificadas como OIV les corresponde aplicar dichas medidas a través de la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) continuo para determinar aquellos riesgos que puedan afectar la seguridad de las redes, sistemas informáticos y datos, y la continuidad operacional de las prestaciones de seguridad social que administra. Dicho sistema, además, deberá permitir evaluar, tanto la probabilidad como el potencial impacto de un incidente de ciberseguridad. Asimismo, las referidas entidades deberán mantener un registro de las acciones ejecutadas que compongan el SGSI, de conformidad a lo que señale el reglamento respectivo.

Las C.C.A.F., deben elaborar e implementar planes de continuidad operacional y ciberseguridad que sean debidamente certificados, en conformidad al artículo 28 de la Ley N°21.663 y sometidos a revisiones periódicas, con una frecuencia mínima de dos años. Asimismo, continuamente realizarán operaciones de revisión, ejercicios, simulacros y análisis de las redes, sistemas informáticos y sistemas para detectar acciones o programas informáticos que comprometan la

ciberseguridad y comunicar la información relativa a dichas acciones o programas al CSIRT Nacional, en la forma que determine el reglamento respectivo.

De conformidad con la Instrucción General N°4, de 2025, de la ANCI las referidas entidades 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 y, además, deberá contar con las certificaciones que señala el artículo 28 de la Ley N°21.663.

Por otro lado, deberá entregar información veraz, suficiente y oportuna a los potenciales afectados, en la medida que puedan identificarse y cuando así lo requiera la ANCI, sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente su información o redes y sistemas informáticos, especialmente cuando involucran datos personales y no exista otra disposición legal que requiera su notificación; o cuando sea necesario para prevenir la ocurrencia de nuevos incidentes o para gestionar uno que ya hubiera ocurrido.

Finalmente, deberán designar a uno o más delegados de ciberseguridad y encargados de reportar, conforme a los numerales 6.1.12.2.2. y 6.1.12.2.3. siguientes y contar con programas de capacitación, formación y educación continua de sus trabajadores y colaboradores, que incluyan campañas de ciberhigiene.

La Política de Seguridad de la Información que elaboren e implementen las C.C.A.F., en el marco de la certificación del SGSI, deberá ser reportada a la Superintendencia de Seguridad Social, para su conocimiento, a través del Sistema GRIS.

6.1.12.2.2. DELEGADO DE CIBERSEGURIDAD

Las C.C.A.F., designarán al menos a un delegado de ciberseguridad, quien deberá tener formación, certificación o experiencia especializada, en el nivel técnico o profesional, en materia de ciberseguridad, gestión de riesgos tecnológicos, continuidad operacional o disciplinas afines. Para estos efectos, deberán realizar la designación de conformidad con las instrucciones contenidas en la Instrucción General N°3, de 2025, de la ANCI.

El delegado de ciberseguridad desempeñará las siguientes funciones:

a. Actuará como contraparte de la ANCI, pudiendo solicitarle asesoría técnica ante la ocurrencia de incidentes de ciberseguridad que hayan comprometido sus activos informáticos críticos o afectado el funcionamiento de su operación. Además, informará a la máxima autoridad institucional señalada en el literal i) del artículo 8° de la ley.

b. Podrá asesorar a la institución en la elaboración de los programas de capacitación, formación y educación continua de los trabajadores y colaboradores, incluyendo campañas de ciberhigiene.
c. Capacitará al personal de la entidad en temáticas sobre prevención de incidentes de ciberseguridad y acciones ante ciberataques, al menos cada seis meses.
d. Podrá asesorar a la institución en el procedimiento para obtener las certificaciones de ciberseguridad que señala la Ley N°21.663 y las que determine la ANCI.
e. Incluirá en los planes de continuidad operacional y ciberseguridad las mantenciones planificadas que produzcan o pudieren producir indisponibilidad de los sistemas informáticos de la institución.

Para que el delegado de ciberseguridad desempeñe adecuadamente sus funciones, las C.C.A.F., deberán habilitarle un canal de comunicación y reporte directo a la máxima autoridad institucional, otorgarle independencia funcional suficiente para comunicar riesgos, incidentes y brechas de cumplimiento a la autoridad interna, sin interferencias de áreas operativas de la institución que pudiesen comprometer la objetividad de dichas comunicaciones y habilitarlo para representar a la institución ante la ANCI.

Las C.C.A.F. deberán informar a la Superintendencia de Seguridad Social, a través del Sistema GRIS, sobre la designación del delegado de ciberseguridad y sus subrogantes y cualquier modificación que efectúe a dicha designación.

6.1.12.2.3.ENCARGADO DE REPORTAR

Las C.C.A.F. designarán a una o más personas encargadas de reportar los ciberataques e incidentes de ciberseguridad, definidos en el artículo 2° de la referida Ley, al Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) Nacional que puedan tener efectos significativos en los términos del artículo 27 de la Ley N°21.663.

La o las personas encargadas de reportar deberán tener formación o experiencia técnica o profesional en ciberseguridad, serán designados conforme a las Instrucciones Generales N°s 1 y 2, de 2025, de la ANCI y desempeñará, al menos, las siguientes funciones:

a. Mantener una relación fluida con el CSIRT Nacional a través de la plataforma de la ANCI y los otros medios de contacto que esa entidad disponga.
b. Inscribir a la institución en la plataforma de la ANCI, siguiendo las Instrucciones Generales N°s 1 y 2, de 2025, de la ANCI y estará obligado a mantener la confidencialidad de sus credenciales, siendo responsable por su uso indebido, o por su utilización por parte de terceras personas.
c. Podrá colaborar en las funciones del delegado de ciberseguridad.

El encargado de reportar puede ser, además, delegado de ciberseguridad, siempre que cumpla con el perfil exigido para ello en el numeral 6.1.12.2.2.

Las C.C.A.F. deberán informar a la Superintendencia de Seguridad Social, a través del Sistema GRIS, sobre la designación del encargado de reportar y sus subrogantes y cualquier modificación que efectúe a dicha designación.

6.1.12.3. CONTENCIÓN Y MITIGACIÓN DE INCIDENTES DE CIBERSEGURIDAD

6.1.12.3.1. REPORTE DE CIBERATAQUES E INCIDENTES DE CIBERSEGURIDAD

Las C.C.A.F., deben reportar oportunamente a la Superintendencia de Seguridad Social la ocurrencia de un ciberataque o un incidente de ciberseguridad, que no puedan tener efectos significativos, a través del Sistema GRIS, a través de los formularios habilitados para ello. Cuando el hecho reportado implique pérdidas operacionales, de acuerdo con lo establecido en el numeral 6.1.10, de este Compendio, la C.C.A.F. deberá incluir la pérdida en el Registro de Información de Pérdidas Mensual.

Sin embargo, cuando el ciberataque o incidente de ciberseguridad pudiera tener efectos significativos, conforme lo dispone el artículo 27 de la Ley N°21.663, el encargado de reportar, deberá enviar, a través de la ventanilla única, los reportes a que se refiere el artículo 9 de la referida Ley y las actualizaciones sobre la situación que se le requieran, en base a la taxonomía establecida en la Resolución N° 7 exenta, de 2025, de la ANCI. Además, deberán informar al CSIRT Nacional su plan de acción, tan pronto lo hubieren adoptado.

Las C.C.A.F. deberán omitir en los reportes y actualizaciones, todo dato o información personal, conforme a la Ley N°19.628 Para estos efectos, la dirección IP no se considerará dato o información personal.

6.1.12.3.2. ENVÍO DE INFORMACIÓN REQUERIDA POR LA ANCI Y EL CSIRT NACIONAL

Con la finalidad de prevenir la ocurrencia de incidentes de ciberseguridad o gestionar uno que ya hubiera ocurrido, la ANCI, de manera particular, específica y fundada, podrá requerir a las C.C.A.F., que le otorguen acceso a la información estrictamente necesaria para ello, o bien, la entrega del registro de actividades de las redes y sistemas informáticos que permitan comprender detalladamente los incidentes de ciberseguridad que puedan haber ocurrido. La referida información deberá ser remitida en el más breve plazo, con los datos personales debidamente anonimizados, si fuera posible sin entorpecer la gestión de

incidentes y efectuando su tratamiento en estricto cumplimiento de la Ley N°19.628, teniendo presente que la dirección IP no es un dato personal. De todas maneras, podrá entregar la información requerida en calidad de reservada, en virtud del artículo 35 de la Ley N°21.663.

En caso de incidentes de impacto cuya gestión lo haga imprescindible, la ANCI podrá requerir, mediante instrucción del Director o Directora, el acceso a redes y sistemas informáticos de los las C.C.A.F., pero cuando requiera restringir el acceso o uso de redes o sistemas informáticos utilizados para el otorgamiento y tramitación de licencias médicas, deberá actuar conjuntamente con la Superintendencia de Seguridad Social. Ante estos requerimientos, la entidad podrá oponerse o proporcionar todas las facilidades de acceso que sean necesarias, conforme lo dispone la letra k) de la Ley N°21.663.

El mismo procedimiento establecido en el párrafo anterior se aplicará cuando la ANCI requiera el acceso a sistemas informáticos, datos, documentos y demás información que fuere necesaria para el desempeño de sus funciones de supervisión y fiscalización.

Por otro lado, las C.C.A.F. deberán remitir al CSIRT Nacional, cuando lo requiera, la información anonimizada de incidentes de ciberseguridad, las vulnerabilidades encontradas y los planes de acción respectivos para mitigarlos.

Las C.C.A.F. deberán informar a la Superintendencia de Seguridad Social, a través del Sistema GRIS, los requerimientos de información que le efectúe la ANCI o el CSIRT."

2. **SUPRÍMANSE** los anexos N°s 5, 6 y 7 del numeral 6.1.13.

III. INCORPÓRASE AL TÍTULO III, LIBRO VI DEL COMPENDIO DE NORMAS QUE REGULAN A LOS SERVICIOS DE BIENESTAR DEL SECTOR PÚBLICO, EL SIGUIENTE NUMERAL:

"**5. ACCIONES DE CIBERSEGURIDAD DE LOS SERVICIOS DE BIENESTAR DEL SECTOR PÚBLICO**

Los Organismos de la Administración del Estado, de los cuales dependen los Servicios de Bienestar fiscalizados por la Superintendencia de Seguridad Social, son instituciones que prestan servicios calificados como esenciales (PSE), conforme lo dispone el artículo 4° de la Ley N°21.663, por consiguiente, corresponde que los Organismos de la Administración del Estado cumplan las obligaciones que establece dicha Ley."

IV. VIGENCIA

Las instrucciones impartidas por esta Circular comenzarán a regir a partir del 02 de noviembre de 2026.

Sin perjuicio de lo anterior, las instrucciones sobre las certificaciones del artículo 28 de la Ley N°21.663 a que hacen referencia los numerales 2.1. del Compendio de Normas sobre Licencias Médicas, Subsidios de Incapacidad Laboral y Seguro Sanna y 6.1.12.2.1., del Compendio de Normas que Regulan a las Cajas de Compensación de Asignación Familiar, entrarán plenamente en vigencia a partir de la fecha que indique el respectivo reglamento de la ANCI. En el intertanto, la ANCI podrá homologar certificaciones técnicas internacionales o extranjeras sobre ciberseguridad mediante resolución fundada de su Director o Directora.

Asimismo, las instrucciones contenidas en la letra A) del numeral 3, del Compendio de Normas sobre Licencias Médicas, Subsidios de Incapacidad Laboral y Seguro Sanna y en el numeral 6.1.12.3.1., del Compendio de Normas que Regulan a las Cajas de Compensación de Asignación Familiar, entrarán en vigencia cuando se habilite la ventanilla única, previa coordinación con la ANCI. Mientras tanto, las entidades deberán realizar dos notificaciones simultáneas, una a la Superintendencia de Seguridad Social a través del Sistema GRIS o GRIS-LM y otra a la plataforma de reporte de la ANCI.