AU08-2020-02135

CIRCULAR N° 3579

SANTIAGO, 10 DE FEBRERO DE 2021

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

MODIFICA EL TÍTULO I. GOBIERNO CORPORATIVO E INCORPORA EL TÍTULO V. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, AMBOS DEL LIBRO VII. ASPECTOS OPERACIONALES Y ADMINISTRATIVOS, Y MODIFICA EL TÍTULO II. GESTIÓN DE REPORTES E INFORMACIÓN PARA LA SUPERVISIÓN (GRIS), DEL LIBRO IX. SISTEMAS DE INFORMACIÓN. INFORMES Y REPORTES, DEL COMPENDIO DE NORMAS DEL SEGURO SOCIAL DE ACCIDENTES DEL TRABAJO Y ENFERMEDADES PROFESIONALES DE LA LEY N°16.744

La Superintendencia de Seguridad Social, en uso de las atribuciones que le confieren los artículos 2°, 3°, 30 y 38 letra d) de la Ley N°16.395 y el artículo 12 de la Ley N°16.744, ha estimado pertinente impartir instrucciones relacionadas con la definición de un marco regulatorio y de buenas prácticas, referido a materias de seguridad de la información y ciberseguridad, aplicable a los organismos administradores del Seguro de Ley N°16.744, a través de la modificación del Título I. Gobiernos corporativos, e incorporación de un nuevo Título V. Gestión de la Seguridad de la Información, ambos del Libro VII. Aspectos Operacionales y Administrativos, y la modificación del Título II. Gestión de Reportes e Información para la Supervisión (GRIS), del Libro IX. Sistemas de Información. Informes y Reportes, todos del Compendio de Normas del Seguro Social de Accidentes del Trabajo y Enfermedades Profesionales de la Ley N°16.744.

I. MODIFÍCASE EL LIBRO VII. ASPECTOS OPERACIONALES Y ADMINISTRATIVOS, EN LOS SIGUIENTES TÉRMINOS:

1. Reemplázase el segundo párrafo del número 9. Política de seguridad de la información, del Capítulo I. Políticas, Letra E. Políticas, Manuales y Planes, del Título I. Gobierno Corporativo, por el siguiente:

   "Asimismo, se considerará buena práctica que esta política contenga al menos los aspectos especificados en la Letra C, Título V, Capítulo III. Gestión de la Seguridad de la Información, de este Libro.".

2. Agrégase antes de la letra a) Registros de información de eventos, del número 3. Generación de una base de eventos de riesgo operacional, del Capítulo V. Riesgo operacional, Letra B. Gestión específica de los riesgos, del Título IV. Gestión de riesgos financieros y operacionales, lo siguiente:

   "• Eventos vinculados a ciberincidentes, según lo establecido en el Capítulo II. Reporte de ciberincidentes, de la Letra D. Ciberseguridad, Título V. Gestión de la Seguridad de la Información, de este Libro.".

3. Incorpórase el siguiente Título V. Gestión de la seguridad de la información:

   "TÍTULO V. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

   A. Generalidades

      CAPÍTULO I. Alcance de las instrucciones impartidas

      Las presentes instrucciones tienen por objeto establecer un marco regulatorio que comprenda los fundamentos generales de seguridad de la información y ciberseguridad, los que deben ser considerados como buenas prácticas por parte de los organismos administradores del Seguro Social de la Ley N° 16.744, con excepción de aquellas instrucciones en las que se indique expresamente su carácter obligatorio.

      Adicionalmente, se establece el reporte obligatorio de ciberincidentes que ocurran en sus redes, equipos y sistemas y que alcancen los niveles de peligrosidad e impacto establecidos en esta normativa, así como también un reporte anual obligatorio de autoevaluación del estado de la seguridad de la información y ciberseguridad al interior de la organización.

Las instrucciones contenidas en el presente Título serán aplicables a todos los organismos administradores del Seguro de la Ley N° 16.744, entendiendo como tales, las mutualidades de empleadores y el Instituto de Seguridad Laboral.

En el caso del Instituto de Seguridad Laboral, estas disposiciones son complementarias a las impartidas por el Estado de Chile respecto de las instrucciones de seguridad de la información.

CAPÍTULO II. Definiciones

a) Seguridad de la información: Conjunto de medidas preventivas y reactivas de los organismos administradores y sus respectivos sistemas tecnológicos, que tienen por objeto resguardar y proteger la información, asegurando la confidencialidad, integridad, autenticidad y disponibilidad de los datos, continuidad de servicios y protección de activos de información.

b) Ciberseguridad: Conjunto de acciones posibles para la prevención, mitigación, investigación y manejo de las amenazas e incidentes sobre los activos de información, datos y servicios, así como para la reducción de los efectos de los mismos y del daño causado antes, durante y después de su ocurrencia.

c) Ciberincidente: Todo evento que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas o datos informáticos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos por dichos sistemas y su infraestructura, que puedan afectar al normal funcionamiento de los mismos.

d) Gestión de incidentes: Procedimiento para la detección, análisis, manejo, contención y resolución de un incidente de ciberseguridad.

e) Protección de los activos de información: Adoptar las medidas que resguarden la seguridad física de los dispositivos, así como los accesos a éstos. Se entenderá por infraestructura crítica las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción pueden tener una repercusión importante en los trabajadores protegidos, pensionados, empresas adherentes o afiliadas y en las prestaciones preventivas, médicas y económicas que debe brindar el seguro.

f) Continuidad de servicios: Adoptar las medidas que permitan proveer un nivel mínimo de servicio, entendiendo por esto las prestaciones propias del seguro, reduciendo el riesgo de eventos que puedan crear una interrupción o inestabilidad en las operaciones de la entidad hasta niveles aceptables y planificando la recuperación de los servicios de las tecnologías de la información (TI).

g) Autenticación: Proceso utilizado en los mecanismos de control de acceso con el objetivo de verificar la identidad de un usuario, dispositivo o sistema mediante la comprobación de credenciales de acceso.

h) Confidencialidad: Adoptar las medidas necesarias que impidan la divulgación de información a individuos, entidades o procesos no autorizados. A su vez, asegurar

que, en el ambiente interno del organismo administrador, sólo las personas autorizadas dentro de ésta tengan acceso a la información.

i) Integridad: Adoptar las medidas necesarias que aseguren que los datos están protegidos de modificaciones no autorizadas y que dichos datos mantienen exactitud respecto del origen de los mismos.

j) Disponibilidad: Adoptar las medidas necesarias que permitan que la información esté a disposición de quienes la necesitan, entendiendo por esto a trabajadores protegidos, pensionados, trabajadores de los organismos administradores, procesos o aplicaciones, Superintendencia de Seguridad Social y otras entidades con competencia en materias del Seguro de la Ley N° 16.744.

B. Responsabilidades del organismo administrador en la gestión de la seguridad de la información

Los organismos administradores deberán implementar medidas técnicas y de organización para gestionar los riesgos de seguridad de la información y ciberseguridad de las redes, equipos y sistemas que utilizan para la administración del Seguro de la Ley N° 16.744, especialmente en lo referente al otorgamiento de las prestaciones médicas, económicas y preventivas a los trabajadores, pensionados y entidades empleadoras adheridas y afiliadas.

El organismo administrador determinará las medidas de gestión que garanticen la disponibilidad, integridad y confidencialidad de la información, de conformidad con la complejidad de sus operaciones, los riesgos asociados, la tecnología disponible y la normativa vigente.

Para establecer un adecuado sistema de gestión de seguridad de la información, se recomienda que el organismo administrador, considere los siguientes aspectos:

a) Contar con una política de seguridad de la información y ciberseguridad definida al interior del organismo administrador, establecida por el Directorio o la Dirección Institucional.

b) Realizar un levantamiento de los activos de información críticos existentes en el organismo administrador asegurando que la información reciba el nivel de protección adecuado de acuerdo con su importancia para la organización. En particular aquellos sistemas relevantes para el soporte de las operaciones y procesos críticos que involucran el adecuado otorgamiento de las prestaciones de seguridad social, con el fin de resguardar la información interna, así como también la de carácter externa relacionada a los trabajadores protegidos, a las entidades empleadoras adheridas o afiliadas, pensionados, entre otros.

c) Conocer los riesgos críticos de las tecnologías de la información identificando los que afecten la seguridad de la información y ciberseguridad.

d) Establecer anualmente el nivel de riesgos aceptado por el organismo administrador en materia de tecnologías de información, considerando además los niveles de disponibilidad mínimos para asegurar la continuidad operacional.

e) Informar al directorio y a toda la organización respecto a los lineamientos principales de la entidad frente a la seguridad de la información.

f) Adoptar las recomendaciones entregadas por auditores externos e internos respecto de esta materia.

g) Contar con el apoyo del área de riesgos existente, procurando que dicha área se involucre en materia de valorización, identificación, tratamiento y tolerancia de los riesgos propios del ambiente de tecnologías de la información a los que se expone el organismo administrador por los distintos factores en que se desenvuelve.

h) Identificar las amenazas más relevantes a las que se expone el organismo administrador ante eventuales ciberataques y evaluar el impacto organizacional que conlleva la vulnerabilidad e indisponibilidad de estos activos de información.

i) Mantener un registro formalmente documentado de los sistemas de información existentes al interior de la organización, señalando el proceso de negocio que gestiona el área usuaria, identificación de la base de datos y sistema operativo que soporta el aplicativo.

C. Elementos de la gestión del sistema de seguridad de la información

CAPÍTULO I. Consideraciones

Para una efectiva gestión del sistema de seguridad de la información, éste se debe integrar a los procesos de los organismos administradores, considerando sus aspectos en el diseño de los procesos y controles establecidos, en base a las obligaciones y responsabilidades derivadas de la administración del Seguro de la Ley N° 16.744.

El sistema de gestión de la seguridad de la información debe ser consistente con las definiciones y objetivos de la política de gestión integral de riesgos, establecida en la Letra A, Título IV, de este Libro, y la política de seguridad de la información a la que se refiere el número 9, Capítulo I, Letra E, del Título I, de este Libro.

CAPÍTULO II. Política de Seguridad de la Información

Para una eficiente gestión del sistema de seguridad de la información, se estima necesario establecer las políticas internas que entreguen el marco en que el organismo administrador gestionará la seguridad de la información.

En dicho contexto, esta política debiese considerar al menos los siguientes aspectos:

a) Definición de la seguridad de la información, objetivos generales, alcance y la importancia de ésta como un mecanismo que permita compartir y gestionar información de forma segura.

b) Una declaración de la intención de la alta administración, que apoye los objetivos y principios de la seguridad de la información, en concordancia con las metas y estrategias del organismo administrador.

c) Una explicación de los principios, estándares y requisitos de cumplimiento más relevantes para el organismo administrador, tales como, el adecuado

otorgamiento de las prestaciones de la Ley N°16.744, cumplimientos normativos de la Seguridad Social, gestión de la continuidad de negocio, consecuencia de una violación de la política de seguridad de la información, entre otros aspectos.

d) Una definición clara respecto de las responsabilidades generales y específicas de la alta gerencia y demás estamentos relevantes dentro del organismo administrador.

e) Considerar un registro de incidentes de seguridad de la información.

f) Referencia de documentos complementarios a la política de seguridad de la información, si corresponde, tales como procedimientos o manuales detallados con reglas o estándares asociados a actividades específicas.

La política de seguridad de la información debiese ser comunicada y difundida a toda la organización, de forma clara y comprensible para el usuario final. Se recomienda considerar, como parte de este proceso, que al momento de la contratación de un colaborador, éste firme que ha tomado conocimiento de dicha política.

La política de seguridad de la información debiese ser revisada y actualizada anualmente, para asegurar que se encuentre en concordancia con las metas y estrategias de los organismos administradores. Este hecho debiese quedar documentado con la correspondiente firma en el control de cambios del referido documento.

CAPÍTULO III. Gestión de riesgos de las tecnologías de la información

La gestión de los riesgos de las tecnologías de la información implica identificar, analizar, evaluar, tratar, monitorear y comunicar el impacto de los riesgos de las tecnologías de la información sobre los procesos de los organismos administradores.

Una vez que se identifiquen los riesgos y se determine el apetito de riesgo, se recomienda especificar la estrategia de gestión de riesgos, asignando un responsable por cada riesgo identificado y, dependiendo de su importancia e impacto, definir cómo tratar el riesgo, es decir, evitar, mitigar, transferir o aceptar dicho riesgo.

Por otra parte, se recomienda que los criterios de tratamiento del riesgo estén especificados y formalizados, y que éstos sean revisados anualmente por la alta administración y el directorio, dejándose registro de dicha actividad.

La identificación y formalización de los riesgos de tecnologías de la información y actividades que contemplan el uso, transporte o almacenamiento de activos de información que impiden cumplir con el objetivo de mantener la confiabilidad, integridad y disponibilidad de los datos, continuidad de servicios y protección de dichos activos de información se realizará en la correspondiente matriz de riesgo y controles, contenida en el número 2, Capítulo V, Letra B, del Título IV, de este Libro, identificando claramente los riesgos que los organismos administradores asocian a los riesgos de seguridad de la información.

De igual forma, se recomienda que los organismos administradores adopten las medidas adecuadas para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten la seguridad de sus redes, equipos y sistemas, con el

objeto de garantizar su continuidad operativa, así como la continuidad de la seguridad de la información. En todos los casos, se podrá diseñar, implementar, practicar y evaluar un plan de respuesta que otorgue adecuada cobertura a sus redes, equipos y sistemas, en conformidad con estándares internacionales o nacionales, de amplia aplicación y, a su vez, desde el punto de vista de los grupos de interés, garantizar la integridad, disponibilidad y confidencialidad de la información.

CAPÍTULO IV. Acceso a programas y datos

En atención a que los procesos de otorgamiento de las prestaciones de los organismos administradores se encuentran vinculados a un sistema de información, el que se compone por un sistema operativo, una base de datos y el aplicativo en sí, para una correcta gestión de la seguridad de la información es recomendable considerar los siguientes aspectos mínimos en la seguridad de acceso a programas y datos:

a) Seguridad de acceso físico tanto a los servidores como a la inmediación o a cualquier centro sobre el que se encuentre información sensible del organismo administrador, empresas adheridas o afiliadas, trabajadores protegidos y otros beneficiarios, emplazando y protegiendo los equipos para reducir las amenazas y peligros ambientales.

b) Identificación y autenticación de reglas de accesos a los sistemas de información mediante usuarios individualizados y contraseñas encriptadas.

c) La administración de accesos a las cuentas de usuarios con privilegios de administrador debe estar formalmente definida e identificada, tanto en la base de datos, sistema operativo que soporta el aplicativo y el aplicativo en sí.

d) Existencia de un procedimiento de creación de cuentas de usuarios con acceso a los sistemas formalmente documentado, que considere las autorizaciones necesarias y perfiles de accesos para los sistemas de información.

e) Monitoreo de accesos periódicos a los sistemas de información, con el objeto de identificar accesos no autorizados o sospechosos.

f) Implementación de controles para garantizar el acceso autorizado a los usuarios, evitando el acceso no autorizado a los sistemas, aplicaciones y servicios.

Los aspectos señalados precedentemente deben ser formalmente documentados en el procedimiento de administración de accesos a los sistemas críticos para las prestaciones del Seguro de la Ley N° 16.744. Asimismo, se recomienda que dicho procedimiento sea revisado y actualizado anualmente, y que se someta a aprobación de la alta gerencia.

CAPÍTULO V. Cambios a programas y datos

Los sistemas utilizados por los organismos administradores para el otorgamiento de las prestaciones del Seguro de la Ley N° 16.744, pueden corresponder a desarrollos internos o externos y, de la misma manera, su administración puede ser propia o tercerizada. Dichos sistemas no deben permitir cambios directos en los ambientes

productivos, y éstos deben encontrarse autorizados tanto por el área de tecnología como por el dueño del proceso.

Para el cumplimiento de lo señalado en párrafo anterior, se recomienda que los organismos administradores consideren al menos los siguientes aspectos:

a) Implementar ambientes de desarrollo y prueba separados del ambiente productivo para los sistemas de información que soportan procesos críticos.

b) Formalizar y documentar los hitos de conformidad y autorización frente a un cambio en los sistemas, tanto del área dueña del proceso como del área de tecnología.

c) Considerar como parte del proceso de cambios a los sistemas, la documentación de las pruebas de usuario y la respectiva conformidad.

Los aspectos antes señalados deben ser formalmente documentados en el procedimiento de gestión de cambio de los sistemas críticos para las prestaciones del Seguro de la Ley N° 16.744, considerando una revisión y actualización anual.

Conjuntamente con lo anterior, se deberá garantizar que la seguridad de la información sea una parte integral de los sistemas de información en todo el ciclo de vida de los datos, incluyendo a los sistemas que proporcionan servicios en redes públicas.

CAPÍTULO VI. Respaldo y restauración de los sistemas

Se recomienda que los organismos administradores implementen medidas de respaldo de la información, restauración de los sistemas, plan de continuidad operacional, además de considerar otras acciones destinadas a mantener el funcionamiento óptimo de los sistemas, y el adecuado otorgamiento de las prestaciones del Seguro de la Ley N° 16.744.

En relación con lo anterior, los organismos administradores debiesen considerar al menos los siguientes documentos:

a) Procedimiento de respaldo y restauración de los sistemas críticos para las prestaciones del Seguro de la Ley N° 16.744. En este documento se debe contemplar al menos, la definición del medio de respaldo, la frecuencia en que éstos se llevarán a cabo según el sistema asociado, el lugar de resguardo de dicha información y el responsable de ejecutar el respaldo. Asimismo, se debe incluir la definición del responsable y la frecuencia de las pruebas de restauración de la información para los sistemas críticos de dicho Seguro.

b) Plan de continuidad operacional, considerando lo instruido en el número 4, del Capítulo V, Letra B, Título IV, del presente Libro.

c) Plan de administración de incidentes, en el que se detalle paso a paso cómo se debe proceder frente a una contingencia o desastre asociado a los servidores o sistemas. Éste debe contener los responsables de iniciar el plan de acción, cargo y datos de contacto, y el procedimiento para documentar y respaldar el evento, así como las condiciones que darán conformidad para finalizar el plan.

CAPÍTULO VII. Responsabilidad y seguridad de los datos

Los organismos administradores deben contar con mecanismos de control que aseguren la exactitud y calidad de los datos y reportes generados, incluida la reportería a los sistemas de información de administración de la Superintendencia de Seguridad Social.

Es responsabilidad de los organismos administradores asegurar que los datos reportados a los sistemas de la Superintendencia de Seguridad Social, sean consistentes, asegurando su totalidad, exactitud e integridad.

Los organismos administradores deberán incorporar en el plan anual de auditoría interna, la revisión sobre la consistencia de los datos reportados a los sistemas de información de la Superintendencia de Seguridad Social.

Por otra parte, se recomienda que, como parte de sus actividades preventivas, los organismos administradores apliquen técnicas de hacking ético, para encontrar vulnerabilidades o fallas de seguridad en el sistema y, de esta manera, adoptar todas las medidas necesarias que posibiliten prevenir una catástrofe cibernética, en función del alcance y periodicidad definidos por el organismo administrador.

Respecto a los activos de la organización que se encuentran accesibles a los proveedores, se deberá acordar con éstos un nivel de seguridad de la información y prestación de servicios conforme a la importancia de dichos activos.

D. Ciberseguridad

CAPÍTULO I. Gestión de la ciberseguridad

Se considera buena práctica la designación al interior de la organización de un profesional en calidad de titular y su respectivo suplente, como contraparte formal de la Superintendencia de Seguridad Social, y que sea el responsable de la seguridad de la información y la ciberseguridad, así como del diseño, mantención, seguimiento y notificación de los riesgos de seguridad de la información y ciberseguridad, considerando controles de segregación de deberes y áreas de responsabilidad para reducir las oportunidades de modificación o uso indebido no autorizado o no intencional de los activos de la organización, incluyendo las nuevas formas de trabajo a distancia o teletrabajo.

Es recomendable que el organismo administrador cuente con un equipo de respuesta para la adecuada gestión de la ciberseguridad, con el objeto de identificar los riesgos de afectación de los servicios por causa de ciberincidentes, verificar el cumplimiento eficaz de los respectivos planes de gestión y reportar los ciberincidentes.

Asimismo, los organismos administradores debiesen establecer planes de gestión de riesgos de ciberseguridad, formulados de acuerdo a estándares y directrices que guarden la debida coherencia con las características de las redes, equipos y sistemas críticos utilizados para el otorgamiento de las prestaciones de Seguro de la Ley N° 16.744.

Se recomienda que los planes de gestión de riesgo sean actualizados y sometidos a aprobación del directorio o dirección institucional y conocidos por la alta gerencia de

los organismos administradores, junto con señalar el estado de los riesgos de ciberseguridad, indicadores claves, principales ciberincidentes y planes de acción de mejoras.

Junto a lo anterior, se recomienda que los planes de gestión de riesgo incluyan medidas para la protección de los datos personales y sensibles, en cumplimiento con lo establecido en la Ley N° 19.628.

CAPÍTULO II. Reporte de ciberincidentes

1. Mecanismo de reporte

   Los organismos administradores deberán reportar a la Superintendencia de Seguridad Social todos los ciberincidentes que detecten en sus redes, equipos y sistemas y que alcancen los niveles de peligrosidad e impacto establecidos en las tablas indicadas en los números 2 y 3 del presente Capítulo. En caso que un suceso pueda asociarse con dos o más tipos de incidentes con niveles de peligrosidad o impacto distintos, se le asignará el nivel más alto.

2. Niveles de peligrosidad

   El nivel de peligrosidad determina la potencial amenaza que supondría la materialización de un incidente en las redes, equipos y sistemas del organismo administrador, así como su efecto en la calidad o continuidad en el otorgamiento de las prestaciones del Seguro de la Ley N° 16.744.

   Conforme a sus características, las amenazas son clasificadas con los siguientes niveles de peligrosidad: Crítico, Muy Alto, Alto, Medio y Bajo. El nivel asignado se determinará según se indica en la siguiente tabla:

<table>
<tr><th colspan="3">Nivel de Peligrosidad</th></tr>
<tr><th>Nivel</th><th>Clasificación</th><th>Tipo de incidente</th></tr>
<tr><td>Crítico</td><td>Amenaza Avanzada Persistente</td><td>APT: Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.</td></tr>
<tr><td rowspan="2">Muy alto</td><td>Código dañino</td><td>• Distribución de malware:
Ej: recurso de una organización empleada para distribuir malware.
• Configuración de malware:
Recurso que aloje ficheros de configuración de malware. Ej: ataque de webinjects para troyano.</td></tr>
<tr><td>Intrusión</td><td>• Robo:
Ej: acceso no autorizado a un sistema informático con el fin de conocer sus datos internos, apoderarse de ellos o utilizar sus recursos, acceso no autorizado a Centro de Proceso de Datos.</td></tr>
</table>

Nivel de Peligrosidad		
Nivel	Clasificación	Tipo de incidente
		• Sabotaje: Ej: destrucción, inutilización, de un sistema de tratamiento de información, la destrucción, alteración de datos contenidos en un sistema de tratamiento de información, cortes de cableados de equipos o incendios provocados.
	Disponibilidad del servicio	• Interrupciones: Ej: ataque informático.
Alto	Contenido abusivo	• Pornografía infantil, contenido sexual o violento inadecuado: Ej: Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
	Código Dañino	• Sistema infectado: Ej: Sistema, computadora o teléfono móvil infectado con un rootkit. • Servidor C&C (Mando y Control): Ej: Conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.
	Intrusión	• Compromiso de aplicaciones: Ej: Compromiso de una aplicación mediante la explotación de vulnerabilidades de software, como por ejemplo a través de una inyección de SQL. • Compromiso de cuentas con privilegios: Ej: Compromiso de un sistema en el que el atacante ha adquirido privilegios.
	Intento de Intrusión	Ataque desconocido: Ej: Ataque empleando exploit desconocido.
	Disponibilidad del servicio	• DoS (Denegación de servicio): Ej: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio. • DDoS (Denegación distribuida de servicio): Ej: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
	Compromiso de la información	• Acceso no autorizado a información: Ej: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos. • Modificación no autorizada de información: Ej: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware.

Nivel de Peligrosidad		
Nivel	Clasificación	Tipo de incidente
	Fraude	• Pérdida de datos: Ej: pérdida por fallo de disco duro o robo físico. • Phishing.
Medio	Contenido abusivo	• Discurso de odio: Ej: ciberacoso, racismo, amenazas a una persona o dirigida contra colectivos.
	Obtención de información	• Ingeniería social Ej: mentiras, trucos, sobornos, amenazas. • Explotación de vulnerabilidades conocidas: Ej: desbordamiento de buffer, puertas traseras, cross site scripting (XSS).
	Intrusión	• Intento de acceso con vulneración de credenciales: Ej: intentos de ruptura de contraseñas, ataque por fuerza bruta. • Compromiso de cuentas sin privilegios.
	Disponibilidad del servicio	• Mala configuración: Ej: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto. • Uso no autorizado de recursos: Ej: uso de correo electrónico para participar en estafas piramidales.
	Fraude	• Derechos de autor: Ej: uso, instalación, distribución de software sin la correspondiente licencia. • Suplantación: Ej: suplantación de una entidad por otra para obtener beneficios ilegítimos.
	Vulnerable	• Criptografía débil: Ej: servidores web susceptibles de ataques POODLE/FREAK. • Amplificador DDoS: Ej: DNS openresolvers o Servidores NTP con monitorización monlist. • Servicios con acceso potencial no deseado: Ej: Telnet, RDP o VNC. • Revelación de información: Ej: SNMP o Redis. • Sistema vulnerable: Ej: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.
Bajo	Contenido abusivo	• Spam. • Escaneo de redes:

Nivel de Peligrosidad		
Nivel	Clasificación	Tipo de incidente
		Ej: peticiones DNS, ICMP, SMTP, escaneo de puertos.
	Obtención de información	• Análisis de paquetes (sniffing).
	Otros	• Otros: Todo aquel incidente que no tenga cabida en ninguna categoría anterior.

3. Niveles de impacto

Los posibles niveles de impacto de un ciberincidente se clasifican en Crítico, Muy Alto, Alto, Medio, Bajo o Sin Impacto. El nivel de impacto correspondiente, se asignará usando como referencia la siguiente tabla:

Niveles de impacto de ciberincidentes	
Nivel	Descripción
Crítico	Afecta a sistemas clasificados como confidenciales o que contengan información calificada como datos sensibles de acuerdo a la ley.
	Afecta a más del 50% de los procesos que soportan los sistemas del organismo administrador.
	Interrupción de la prestación del servicio igual o superior a 12 horas o superior al 40% de los beneficiarios del seguro.
	Afecta a más del 50% de sus agencias o centros de atención a nivel nacional.
	Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) afectando a la reputación de terceros.
Muy Alto	Afecta a la seguridad ciudadana con potencial peligro para bienes materiales.
	Afecta la vida privada y/o la honra de la persona y su familia, y asimismo, la protección de sus datos personales.
	Afecta a más del 40% de los procesos que soportan los sistemas del organismo administrador.
	Interrupción de la prestación del servicio igual o superior a 8 horas o superior al 30% de los beneficiarios del seguro.
	Afecta a más del 40% de sus agencias o centros de atención a nivel nacional.
	Daños reputacionales, con eco mediático (amplia cobertura en los medios de comunicación) afectando a la reputación de terceros.
Alto	Afecta a más del 30% de los procesos que soportan los sistemas del organismo administrador.
	Interrupción de la prestación del servicio igual o superior a 6 horas o superior al 20% de los beneficiarios del seguro.
	Afecta a más del 30% de sus agencias o centros de atención a nivel nacional.
	Daños reputacionales, con eco mediático (amplia cobertura en los medios de comunicación) que no afecta la reputación de terceros.
Medio	Afecta a más del 20% de los procesos que soportan los sistemas del organismo administrador.
	Interrupción de la prestación del servicio igual o superior a 4 horas y superior al 10% de los beneficiarios del seguro.
	Afecta a más del 20% de sus agencias o centros de atención a nivel nacional.

Niveles de impacto de ciberincidentes	
Nivel	Descripción
	Daños reputacionales sin eco mediático.
Bajo	Afecta al 10% o más, de los sistemas del organismo administrador.
	Interrupción de la prestación del servicio igual o superior a 2 horas y superior al 5% de los beneficiarios del seguro.
	Afecta al 10% o más, de sus agencias o centros de atención a nivel nacional.
Sin impacto	No hay ningún impacto apreciable.

4. Resolución de ciberincidentes

   Una vez detectado un ciberincidente que afecte a una red, equipo o sistema utilizado en el otorgamiento de las prestaciones del Seguro de la Ley N° 16.744, el organismo administrador deberá efectuar, de manera oportuna, todas las gestiones que sean necesarias para su resolución y restaurar la normal provisión de los servicios afectados, dando primera prioridad a aquellas medidas que permitan evitar o, en su defecto, minimizar el impacto a los grupos de interés.

   En caso que el organismo administrador afectado lo considere necesario, podrá solicitar la colaboración de la Superintendencia de Seguridad Social u otras entidades competentes en materia de ciberseguridad, para la resolución de un ciberincidente.

   Los organismos administradores deberán proporcionar la información adicional que les sea requerida para analizar la naturaleza, causas y efectos de los incidentes notificados, así como para elaborar estadísticas y reunir los datos necesarios para elaborar informes de resultados.

   Asimismo, sin perjuicio de las medidas inmediatas conducentes a la mitigación de los efectos y al restablecimiento de los servicios afectados por un ciberincidente, los organismos administradores deberán subsanar, en la medida que sea técnicamente posible, las vulnerabilidades de sus sistemas, equipos y redes que hubieren permitido o facilitado el ciberincidente.

   En caso que un organismo administrador detecte que sus redes, equipos y sistemas fueron utilizados como medio para la comisión de algún delito informático, éste deberá efectuar las denuncias ante los órganos competentes, ejercer las acciones judiciales pertinentes e informar a la Superintendencia de Seguridad Social.

   Los organismos administradores deberán establecer los protocolos de recuperación de la información, en caso de pérdida de ésta por manipulación, ciberincidentes u otras causas de su responsabilidad.

5. Contenido de los reportes de ciberincidentes

   Los organismos administradores deberán reportar toda aquella información relativa al ciberincidente, cuyo nivel de impacto o peligrosidad, se encuentra definido en los niveles Alto, Muy Alto o Crítico, según lo establecido en los números 2 y 3 del presente Capítulo.

Esta información deberá ser recopilada con la rapidez que amerita, sin afectar la estrategia de contención del incidente y los mecanismos desplegados para evitar la propagación del mismo en la red interna, en la red externa y la interoperación con los beneficiarios y grupos de interés.

Además de la rapidez para obtener la información, se recomienda seguir las buenas prácticas de primera respuesta forense internacionalmente aceptadas o que hayan sido validadas nacionalmente por el Instituto Nacional de Normalización, con el objetivo de contaminar lo menos posible las evidencias que permitan investigaciones avanzadas por parte de equipos de ciberseguridad altamente especializados o los entes persecutores que correspondan.

Sin perjuicio de lo anterior, los organismos administradores deberán mantener una bitácora con el registro de todos los ciberincidentes identificados.

a) Reporte de alerta de ciberincidente

   Dentro del plazo de 1 hora, contado desde la toma de conocimiento del ciberincidente, los organismos administradores deberán reportar al sistema GRIS, a través del documento D.12 “Reporte de alerta de ciberincidente”, conforme a lo establecido en el Anexo N°21 “Reportes de Ciberincidentes”, de la Letra F. Anexos, de este Título, la siguiente información:

   i) Identificación del organismo administrador.

   ii) Resumen ejecutivo del ciberincidente.

   iii) Fecha y hora precisas de detección del ciberincidente.

   iv) Recursos tecnológicos afectados.

   v) Tipo de ciberincidente.

b) Informe parcial de ciberincidente

   Posteriormente, a las 6 horas desde la toma de conocimiento del ciberincidente, los organismos administradores deberán reportar al sistema GRIS, a través del documento D.13 “Informe parcial de Ciberincidente”, conforme a lo establecido en el Anexo N°21 “Reportes de Ciberincidentes”, de la Letra F. Anexos, de este Título, la siguiente información:

   i) Identificación del organismo administrador.

   ii) Resumen ejecutivo del ciberincidente.

   iii) Fecha y hora estimada de ocurrencia del ciberincidente.

   iv) Fecha y hora estimada de detección del ciberincidente.

   v) Descripción detallada de lo sucedido, señalando los activos de información afectados y su nivel de sensibilidad y afectación (confidencialidad/integridad/disponibilidad).

   vi) Recursos tecnológicos afectados.

   vii) Tipo de ciberincidente.

viii) Extensión geográfica, si se conoce.

ix) Sistemas de información afectados actuales y potenciales.

x) Grupos de interés afectados actuales y potenciales.

c) Informe de resolución de Ciberincidente

Finalmente, a los 10 días hábiles desde la toma de conocimiento del ciberincidente, los organismos administradores deberán reportar al sistema GRIS, a través del documento D.14 “Informe de resolución de Ciberincidente”, conforme a lo establecido en el Anexo N°21 “Reportes de Ciberincidentes”, de la Letra F. Anexos, de este Título, la siguiente información:

i) Identificación del organismo administrador.

ii) Resumen ejecutivo del ciberincidente.

iii) Origen o causa identificable del ciberincidente.

iv) Total de sistemas de información afectados.

v) Total de grupos de interés afectados.

vi) Infraestructura crítica afectada.

vii) Descripción de los niveles de compromiso: indicadores de compromiso de nivel IP, indicadores de compromiso de nivel de dominios y subdominios, indicadores de compromiso de correos, indicadores de compromiso a nivel HASH (MD5/SHA1/SHA256 o el que los reemplace), vulnerabilidades facilitadoras del incidente y posibles vectores de ingreso/egreso de los artefactos, y en general los datos técnicos del incidente, entre otros similares.

viii) Descripción del plan de acción y medidas de resolución y mitigación.

ix) Medios necesarios para la resolución calculados en horas hombre (HH) / persona.

x) Impacto económico estimado, si procede y es conocido.

xi) Daños reputacionales, aun cuando sean eventuales.

xii) Descripción cronológica de los hechos asociados del ciberincidente.

E. Reporte de Autoevaluación

Los organismos administradores deberán realizar anualmente una autoevaluación del estado de la seguridad de la información y ciberseguridad al interior de la organización.

Para esto, se deberá elaborar un informe de autoevaluación de gestión de seguridad de la información y ciberseguridad, conforme a lo establecido en el Anexo N°20 “Informe de autoevaluación de la seguridad de la información”, de la Letra F. Anexos, de este Título.

El informe de autoevaluación deberá ser conocido por el directorio y remitido al sistema GRIS de la Superintendencia de Seguridad Social, a través del archivo "D.15 Informe de autoevaluación de Seguridad de la Información", a más tardar el último día de enero de cada año, referido a la evaluación del año calendario anterior.

F. Anexos

Anexo N°20 "Informe de autoevaluación de la seguridad de la información".

Anexo N°21 "Reportes de Ciberincidentes".

II. INTRODÚCENSE LAS SIGUIENTES MODIFICACIONES A LA LETRA C. ANEXOS, DEL TÍTULO II. GESTIÓN DE REPORTES E INFORMACIÓN PARA LA SUPERVISIÓN (GRIS), DEL LIBRO IX:

1. Agrégase en el Anexo N° 30 "Formato de los archivos del sistema GRIS", al final de la tabla D. Informes, las siguientes nuevas filas de los documentos "D.12", "D.13", "D.14" y "D.15":

D.12	Reporte de alerta de Ciberincidente	Alerta_ciberincidente
D.13	Informe parcial de Ciberincidente	Informe_parcial_Ciberincidente
D.14	Informe de resolución de Ciberincidente	Informe_resolución_Ciberincidente
D.15	Informe de autoevaluación de Seguridad de la Información	Informe_seguridad_Información

2. Intercálase en el Anexo N° 31 "Calendario de envío de los archivos del sistema GRIS", letra B), las siguientes nuevas filas de los documentos "D.12", "D.13", "D.14" y "D.15", entre las actuales filas de los documentos "D.11" y "E.1":

D.12	Reporte de alerta de Ciberincidente	Permanentemente actualizado	Dentro del plazo de 1 hora contado desde la toma de conocimiento del ciberincidente.
D.13	Informe parcial de Ciberincidente	Permanentemente actualizado	Hasta 6 horas contadas desde la toma de conocimiento del ciberincidente.
D.14	Informe de resolución de Ciberincidente	Permanentemente actualizado	Hasta 10 días hábiles, contado desde el día de la toma de conocimiento del ciberincidente.

D.15	Informe de autoevaluación de Seguridad de la Información	Anual	Hasta el último día del mes de enero de cada año.

III. VIGENCIA

Las modificaciones introducidas por la presente circular, entrarán en vigencia a partir del 1° de enero de 2022.

ANA PATRICIA Soto Altamirano

Firmado digitalmente por ANA PATRICIA Soto Altamirano
Fecha: 2021.02.10 20:02:03 -03'00'

PATRICIA SOTO ALTAMIRANO
SUPERINTENDENTA DE SEGURIDAD SOCIAL (S)

GOP/JAA/ETS/RAM/JRO/CGU/FZM
DISTRIBUCIÓN
Mutualidades de Empleadores de la Ley N°16.744
Instituto de Seguridad Laboral
Departamento de Supervisión y Control
Departamento de Regulación
Departamento de Tecnología y Operaciones

ANEXO N° 20

INFORME DE AUTOEVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Para informar acerca de la autoevaluación de Gestión de la Seguridad de la Información, establecida en el Capítulo I, del Título V, del Libro VII, del Compendio de Normas del Seguro de la Ley N° 16.744, se ha definido la tabla "Autoevaluación de la Seguridad de la Información" que a continuación se especifica.

El organismo administrador podrá anexar información que considere pertinente para dar mayor nivel de detalle a lo informado.

Los campos específicos a reportar son los siguientes:

a) **Resultado de autoevaluación:** deberá indicar para cada pregunta, el estado en el que se encuentra el cumplimiento de acuerdo a las siguientes opciones:

   i. **Cumple:** El organismo administrador cumple con la implementación de las acciones definidas para el tema especificado.

   ii. **Cumple parcialmente**: El organismo administrador cumple parcialmente con la implementación y ejecución del tema especificado.

   iii. **No cumple:** El organismo administrador no ha implementado ni ejecutado el tema especificado.

b) **Descripción del fundamento de la Autoevaluación:** incluir el fundamento que explique y justifique la evaluación establecida por el organismo administrador.

Tabla: Autoevaluación de la Seguridad de la Información			
#	**Pregunta**	**Resultado de autoevaluación**	**Descripción del fundamento de la autoevaluación**
1	El organismo administrador ha implementado medidas técnicas y de organización para gestionar los riesgos de seguridad de la información y ciberseguridad de las redes, equipos y sistemas que utilizan para el otorgamiento de las prestaciones. Detallar las medidas.		
2	El organismo administrador ha determinado las medidas de gestión que garanticen la disponibilidad, integridad y confidencialidad de la información. Detallar las medidas.		
3	El organismo administrador cuenta con una política de seguridad de la información y ciberseguridad, establecida por el Directorio o la Dirección Institucional.		
4	El organismo administrador ha realizado un levantamiento de los activos de información críticos.		

	Adjuntar documento con el levantamiento de los activos de información.		
5	El organismo administrador ha identificado los riesgos críticos de las tecnologías de la información, individualizando aquellos que afecten la seguridad de la información y ciberseguridad. Adjuntar los riesgos identificados.		
6	El organismo administrador ha establecido formalmente el nivel de riesgos aceptado en materia de tecnologías de Información, considerando además los niveles de disponibilidad mínimos para asegurar la continuidad operacional. Aportar documento de respaldo.		
7	El organismo administrador ha designado a un responsable del diseño, mantención y seguimiento de los riesgos de seguridad de la información y ciberseguridad. Señalar al designado responsable (nombre y cargo).		
8	El organismo administrador ha creado un registro formalmente documentado de los sistemas de información existentes al interior de la organización, señalando que proceso de negocio gestiona, el área usuaria, identificación de la base de datos y sistema operativo que soporta el aplicativo. Aportar documento de respaldo.		
9	Los criterios de tratamiento del riesgo se encuentran especificados y formalmente documentados. Adjuntar documento correspondiente.		
10	El organismo administrador ha implementado medidas asociadas a la seguridad de acceso físico tanto a los servidores como a la inmediación o a cualquier centro sobre el que se encuentre información sensible. Detallar medidas.		
11	El organismo administrador ha implementado reglas de accesos (identificación y autenticación) a los sistemas de información mediante usuarios individualizados y contraseñas encriptadas.		
12	Las cuentas de usuarios con privilegios de administrador se encuentran formalmente definidas e identificadas, tanto en la base de datos, sistema		

	operativo que soporta el aplicativo y el aplicativo en sí. Aportar detalle.		
13	Existe un procedimiento formalmente documentado que considere las autorizaciones necesarias y perfiles de accesos para los sistemas de información. Aportar documento.		
14	Se ha implementado un monitoreo de accesos periódicos sobre los sistemas con el objeto de identificar accesos no autorizados o sospechosos a los sistemas de información. Aportar informe de resultados.		
15	Se han implementado ambientes de desarrollo y prueba separados del ambiente productivo para los sistemas de información que soportan procesos críticos del organismo administrador.		
16	Se encuentran formalizados y documentados los hitos de conformidad y autorización frente a un cambio en los sistemas, tanto del área dueña del proceso así como también la contraparte técnica.		
17	Se considera como parte del proceso de cambios a los sistemas, la documentación de las pruebas de usuario y la respectiva conformidad. Aportar documento de ejemplo.		
18	Existe un procedimiento formalmente documentado de control y gestión de cambio a los sistemas y datos. Aportar documento.		
19	Existe un procedimiento formalmente documentado de procedimiento de respaldo y restauración de los sistemas críticos. Aportar documento.		
20	Existe un plan formalmente documentado de administración de ciberincidentes. Aportar documento.		
21	El organismo administrador ha considerado en el plan anual de auditoría interna la revisión sobre la consistencia de los datos reportados a los sistemas de información de administración de esta Superintendencia. Aportar informe de resultados.		
22	El organismo administrador ha definido la ejecución de un hacking ético periódicamente. Aportar si aplica.		

ANEXO N° 21
REPORTES DE CIBERINCIDENTES

A) Reporte de Alerta de Ciberincidente

Organismo Administrador
Resumen ejecutivo del ciberincidente
Fecha y hora precisas de detección del ciberincidente
Recursos tecnológicos afectados
Tipo de ciberincidente (ver Capitulo II Reporte de ciberincidentes, tabla Nivel de Peligrosidad)

B) Informe parcial de Ciberincidente

Organismo Administrador
Resumen ejecutivo del ciberincidente
Fecha y hora precisas de ocurrencia del ciberincidente
Fecha y hora precisas de detección del ciberincidente
Descripción detallada de lo sucedido, señalando los activos de información afectados y su nivel de sensibilidad y afectación (confidencialidad/integridad/disponibilidad)

Recursos tecnológicos afectados
Tipo de ciberincidente (ver Capitulo II Reporte de ciberincidentes, tabla Nivel de Peligrosidad)
Extensión geográfica, si se conoce
Sistemas de información afectados actuales y potenciales
Grupos de interés afectados actuales y potenciales

C) Informe de resolución de ciberincidente

Organismo Administrador
Resumen ejecutivo del ciberincidente
Origen o causa identificable del ciberincidente
Total de sistemas de información afectados
Total de grupos de interés afectados
Infraestructura crítica afectada

Descripción de los niveles de compromiso
Descripción del plan de acción y medidas de resolución y mitigación
Medios necesarios para la resolución calculados en horas hombre (HH) / persona
Impacto económico estimado, si procede y es conocido
Daños reputaciones, aun cuando sean eventuales
Bitácoras generadas de forma automática por los sistemas