Departamento de Transparencia y Documentación - Instituto de Previsión Social
Avenida del Lib. Bernardo O'Higgins Nº 1353 - Santiago
Teléfonos [redacted] www.ips.gob.cl

APRUEBA LA "POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN" INSERTA EN EL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO DE PREVISIÓN SOCIAL, APROBADA POR RESOLUCIÓN EXENTA N° 657, DE 2015.

RESOLUCIÓN EXENTA N° 223

SANTIAGO, 18 MAY 2016

VISTOS:

1.- La Ley N° 20.255, de Reforma Previsional, que establece la nueva Institucionalidad Pública para el Sistema de Previsión Social y crea entre sus órganos, el Instituto de Previsión Social determinando sus funciones y atribuciones; y el D.F.L. N° 4, de 2009, del Ministerio del Trabajo y Previsión Social que fija la Planta de Personal y fecha de iniciación de actividades de este Instituto.

2.- El D.F.L.N°1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fijó el texto refundido, coordinado y sistematizado, de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

3.- La Ley N° 19.880, de Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado.

4.- El D.S. N° 83, de 2005, del Ministerio Secretaría General de la Presidencia, que aprueba la Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confiabilidad de los Documentos Electrónicos; y el Decreto N° 100, de 2006, de la misma cartera ministerial, que aprueba la norma técnica para el desarrollo de Sitios Web de los Órganos de la Administración del Estado.

5.- La Ley N° 19.799, sobre firma y documentos electrónicos y su Reglamento contenido en el D.S. N° 181, de 2002, del Ministerio de Economía, Fomento y Reconstrucción.

6.- El D.F.L. N° 278, de 1960, del Ministerio de Hacienda; el D.L. N° 49, de 1973; el D.F.L. N° 17, de 1989, del Ministerio del Trabajo y Previsión Social; la Resolución N° 1600, de 2008, de la Contraloría General de la República, que fijó las normas sobre exención del trámite de toma de razón; y las facultades que me concede el artículo 57°, de la Ley N° 20.255.

Departamento de Transparencia y Documentación – Instituto de Previsión Social
Avenida del Lib. Bernardo O'Higgins Nº 1353 – Santiago
Teléfonos [redacted] www.ips.gob.cl

CONSIDERANDO:

1.- Que, por Resolución Exenta N° 591, de 28 de diciembre de 2009, de la Dirección Nacional de este Instituto de Previsión Social, se aprobaron los documentos asociados a la "Política de Seguridad de la Información del IPS" y "Política de Gestión de Incidentes de Seguridad de la Información", instrumento modificado por la Resolución Exenta N° 83, de 10 de febrero de 2011, para los efectos de incorporar los textos de la "Política de Desarrollo y Mantenimiento de Sistemas" y "Política de Gestión de Continuidad de Negocio", todos los cuales resultan aplicables a todos los procesos de Seguridad del Instituto de Previsión Social y que respectivamente, forman parte integrante de dichos actos administrativos.

2.- Que, a través de Resolución Exenta N° 523, de 29 de octubre de 2012, se dispone una nueva constitución del Comité de Seguridad del Instituto de Previsión Social, integrado por los funcionarios que desempeñan los cargos que singulariza y dispone lo que indica.

3.- Que, mediante Resolución Exenta N°170, de 10 de abril de 2015, esta Dirección Nacional designa a la encargada de Seguridad del Instituto de Previsión Social, con dependencia de la Subdirección de Sistemas de la Información y de Administración de este Instituto.

4.- Que, por Resolución Exenta N° 657, de 03 de diciembre de 2015, esta Dirección Nacional aprueba para este Instituto la "Política General de Seguridad de la Información" y en su Resuelvo N° 2, deja sin efecto el Resuelvo N°1 y el Resuelvo N°2, punto N°1, "Documento Política General de Seguridad de la Información" y "Documento Preliminar sobre Política de Seguridad, de la Resolución Exenta N°591, de 28 de diciembre de 2009, singularizada en el Considerando N° 1, del presente instrumento.

5.- Que, en el contexto indicado, la Encargada de Seguridad de la Información, ha elaborado el texto denominado **"Política de Gestión de Incidentes de Seguridad de la Información"**, cuyo proyecto ha sido revisado por el Jefe de la División Informática, el Jefe de la División Planificación y Desarrollo de este Instituto.

6.- Que, asimismo por Oficio Ordinario N°44172/1345-16, de 22 de marzo de 2016, complementado por Oficio Ordinario N°44172/1846-16, de 19 de abril del mismo año, la División Jurídica de este Instituto, aprueba y visa en cada una de sus páginas el proyecto denominado **"Política de Gestión de Incidentes de Seguridad de la Información"**, aprobado por el Comité de Seguridad de la Información, en sesión de 06 de enero de 2016, acogiendo además, las adecuaciones formuladas por la Encargada de Seguridad de la Información al texto del mismo, mediante documento electrónico de 07 de abril de 2016, estableciendo la procedencia de emitir la Resolución aprobatoria de rigor, la que por su naturaleza se encuentra exenta del trámite de toma de razón, por la Contraloría General de la República.

RESUELVO:

1.- Apruébase, para el Instituto de Previsión Social la **"Política de Gestión de Incidentes de Seguridad de la Información"**, que consta de diez (10) páginas, que se adjunta como parte integrante de la presente Resolución Exenta, con aprobación legal de fecha 19 de abril de 2016, cuyos objetivos se indican a continuación:

Departamento de Transparencia y Documentación – Instituto de Previsión Social
Avenida del Lib. Bernardo O'Higgins Nº 1353 – Santiago
Teléfonos [redacted] www.ips.gob.cl

- Asegurar que la ocurrencia de eventos y debilidades detectados en los sistemas de seguridad de información, implique una relación entre ellos que genere acciones preventivas oportunas, así como las necesarias de carácter correctivo.
- Establecer un método y enfoque consistente y eficaz en la gestión de los incidentes de seguridad de la información.
- Definir el alcance, marco de referencia y responsabilidades, respecto de la notificación, registro y gestión de los incidentes de seguridad de la información, que afectan la disponibilidad, integridad y confidencialidad de los activos de información.

2.- Publíquese el Procedimiento, que se aprueba por el presente acto administrativo, en el ambiente "Instructivos Institucionales", de la Intranet del IPS.

Notifíquese, regístrese y distribúyase por Departamento de Transparencia y Documentación, a las Jefaturas de las unidades incluidas en la Distribución de la presente Resolución.

INSTITUTO DE PREVISIÓN SOCIAL

PATRICIO CORONADO ROJO
DIRECTOR NACIONAL
INSTITUTO DE PREVISIÓN SOCIAL

DISTRIBUCION:
- Gabinete Dirección Nacional
- Subdirección de Servicios al Cliente
- Subdirección de Sistema de Información y de Administración
- División Jurídica
- División Contraloría Interna
- División Beneficios
- División Canales de Atención a Clientes
- División Informática
- División Planificación y Desarrollo
- Departamento Auditoría Interna
- Departamento Comunicaciones
- Departamento de Transparencia y Documentación
- Departamento de Finanzas
- Departamento Administración e Inmobiliaria
- Departamento de Personas
- Departamento Cobranza Institucional
- A los Directores Regionales IPS, que deberán comunicar el presente instrumento a los Centros de Atención Previsional Integral de su dependencia
- Unidad Apoyo Documental de la División Jurídica
- A la Encargada de Seguridad del IPS
- Silvana Fuentes Novoa, División Contraloría Interna

MHES/ACA/YGE/VCG/MJEW/NOR/RPY/MRC/mrc
Aprueba "Política de Gestión de Incidentes de Seguridad de la Información".
IV-46 (Folio DTD-3575-84-2)

POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

DIVISIÓN JURÍDICA V°B° DEPTO. CONTROL JURÍDICO I.P.S.

CONTROL DE CAMBIOS

Fecha	Versión	Página	Numeración del contenido	Cambio Efectuado/Nombre del responsable
05/01/2016	01			Versión inicial del documento

(*) La presente versión substituye completamente a todas las precedentes, de manera que este sea el único documento valido de entre todos los de la serie.

CLASIFICACIÓN DEL DOCUMENTO

NIVEL DE CONFIDENCIALIDAD: Uso interno.
NOTA DE CONFIDENCIALIDAD: Documento disponible sólo a funcionarios del IPS.

CONTROL DE DIFUSIÓN

AUTOR/ES: Encargado de Seguridad de la Información
DISTRIBUCIÓN: Funcionarios del IPS

DIVISIÓN JURÍDICA V°B° DEPTO. CONTROL JURÍDICO I.P.S.

CONTROL LEGAL Y NORMATIVO.

República de Chile

- Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, cuyo texto refundido fue fijado por el D.F.L. N° 1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia.
- Ley N° 18.834 Aprueba Estatuto Administrativo, cuyo texto refundido fue fijado por el D.F.L N° 29, de 2004, del Ministerio de Hacienda.
- La Ley N° 19.880, que establece las "Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado".
- Ley Nº 20.285 sobre "Transparencia y Acceso a la Información Pública", y su Reglamento contenido en el Decreto Nº 13, de 2009, del Ministerio Secretaría General de la Presidencia.
- Ley N° 19.628, sobre "Protección de la Vida Privada y Datos Personales", Ministerio Secretaría General de la Presidencia.
- Ley Nº 17.336, sobre "Propiedad Intelectual", Ministerio de Educación.
- Ley Nº 19.223, sobre "Delitos informáticos" del Ministerio de Justicia.
- Decreto Supremo N° 83/2004, del Ministerio Secretaria General de la Presidencia que aprueba norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos.
- Decreto Supremo N° 93/2006 del Ministerio Secretaria General de la Presidencia, Norma Técnica para la Adopción de Medidas destinadas a Minimizar los efectos Perjudiciales de los Mensajes Electrónicos Masivos no solicitados.
- Ley N°19.799, sobre documentos electrónicos, firma electrónica y los servicios de certificación de dicha firma. Ministerio de Economía.
- Ley 18.168, Ley General de Telecomunicaciones.
- Ley 19.927, Modifica el Código Penal, el Código de Procedimiento Penal y el Código Procesal Penal en Materia de Delitos de Pornografía Infantil.
- Decreto 779, noviembre 2000, reglamento del registro de bancos de datos personales a cargo de organismos públicos.
- Decreto 277. Reglamento de Propiedad Intelectual.
- Ord., Nº 1902-229 del 23/12/2011, del Director Nacional, que imparte instrucciones programáticas en materia de Gestión de Seguridad de la Información con el objeto que las jefaturas tomen medidas pertinentes en relación al personal de su dependencia o que se desempeñe en sus unidades dependientes.
- Resolución Exenta N° 170, de 10 de abril de 2015, que designó al Encargado de Seguridad de la Información.
- OS N°181/2002 del Ministerio de Economía, Fomento y Reconstrucción Reglamento Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma.

DIVISIÓN JURÍDICA V°B° DEPTO. CONTROL JURÍDICO I.P.S.

República de Chile
• Instructivo Presidencial N° 05, mayo de 2001: Define el concepto de Gobierno Electrónico. Contiene la mayor parte de las instrucciones referidas al desarrollo de Gobierno Electrónico en Chile. • Instructivo Presidencial N° 06, junio de 2004: Imparte instrucciones sobre la implementación de la firma electrónica en los actos, contratos y cualquier tipo de documento en la administración del Estado, para dotar así de un mayor grado de seguridad a las actuaciones gubernamentales que tienen lugar por medio de documentos electrónicos y dar un mayor grado de certeza respecto de las personas que suscriben tales documentos. • Instrucción General N°2, mayo de 2009, del Consejo para la Transparencia: Designación de Enlaces con el Consejo para la Transparencia. • Instrucción General N°3, mayo de 2009, del Consejo para la Transparencia: Índice de Actos o Documentos calificados como secretos o reservados. • Instructivo Presidencial N°08, diciembre de 2006: Imparte instrucciones sobre Transparencia Activa y Publicidad de la Información de la Administración del Estado. • Circular N° 3, enero de 2007, del Ministerios del Interior y Hacienda: Detalla las medidas específicas que deben adoptar los servicios y dispone los materiales necesarios para facilitar la implementación del instructivo presidencial sobre transparencia activa y publicidad de la información de la Administración del Estado. • Instructivo Presidencial N°4, junio de 2003: Imparte instrucciones sobre aplicación de la Ley de Bases de Procedimientos Administrativos.

REFERENCIAS

Documentos Internos	
Titulo	**Nombre del archivo**
Política General de Seguridad de la Información	Política General de Seguridad de la información.doc
Manual Proceso de Inducción	Manual Proceso de Inducción.doc

DIVISIÓN JURÍDICA V°B° DEPTO. CONTROL JURÍDICO I.P.S.

Otros Documentos	Norma ISO: NCh-ISO 27001:2013
	A.16.1.1 Responsabilidades y procedimientos A.16.1.2 Informe de eventos de seguridad de la información A.16.1.3 Informe de las debilidades de seguridad de la información A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de la información A.16.1.5 Respuesta ante incidentes de seguridad de la información A.16.1.6 Aprendizaje de los incidentes de seguridad de la información A.16.1.7 Recolección de evidencia

NOTA:

El uso de un lenguaje que no discrimine ni marque diferencias entre hombres y mujeres ha sido una preocupación en la elaboración de este documento. Sin embargo, y con el fin de evitar la sobrecarga gráfica que supondría utilizar en español o/a para marcar la existencia de ambos sexos, se ha optado por utilizar el masculino genérico, en el entendido de que todas las menciones en tal género representan siempre a todos/as, hombre y mujeres, abarcando claramente ambos sexos.

DIVISIÓN JURÍDICA V°B° DEPTO. CONTROL JURÍDICO I.P.S.

ÍNDICE

1. OBJETIVO

Asegurar que la ocurrencia de eventos y debilidades detectados en los sistemas de seguridad de información , que relacionados entre ellos, generen acciones preventivas oportunas, así como las necesarias de carácter correctivo.
Establecer un método y enfoque consistente y eficaz en la gestión de los incidentes de seguridad de la información.
Definir el alcance, marco de referencia y responsabilidades, respecto de la notificación registro y gestión de los incidentes de seguridad de la información, que afectan la disponibilidad, integridad y confidencialidad de los activos de información.

2. ALCANCE

Incluye todo evento o incidente que afecte negativamente los activos de información o los procesos de negocio con los que están relacionados. Se aplica a todos los activos de información con los que el IPS cuente en la actualidad o a los que adquiera en el futuro.
Dirigida a todos los funcionarios de IPS, y personal externo, responsables de administrar información, o procesos del negocio para la continuidad del servicio.

3. DEFINICIONES

Incidente de seguridad: Situación adversa que amenaza o pone en riesgo un proceso en el que exista tratamiento de datos, independientemente de su grado de confidencialidad.

Activo de Información: Elementos más relevantes para la producción, el procesamiento, la emisión, el almacenaje, la comunicación, la visualización, los encargados y la recuperación de la información que tiene un elevado valor para la organización. Pueden clasificarse en personas, sistemas, hardware e infraestructura.

Comité de Seguridad de la Información: Es un comité integrado por las Jefaturas de División del Instituto así como por ciertas jefaturas de departamentos, involucrados en los temas informáticos. Es presidido por el Encargado de Seguridad de la Información y su objetivo principal es tomar decisiones que apunten a la mejora de los controles y a adoptar las medidas correctivas pertinentes.

Continuidad del negocio: Se refiere a la mantención de los procesos institucionales ante un incidente que pueda afectarlos.

DIVISIÓN JURÍDICA V°B° DEPTO. CONTROL JURÍDICO I.P.S.

Plan de Continuidad: Es un plan de emergencia con el objetivo de mantener la funcionalidad de la organización a un nivel mínimo aceptable durante una contingencia.

Custodio de la Información: Corresponde al funcionario que mantiene bajo su responsabilidad, información de la que no es propietario, pero que por su cometido se encuentra encargado de aplicar las medidas de seguridad que se definan de acuerdo a su valor.

Encargado de seguridad de la Información: Funcionario que supervisa la correcta aplicación de los manuales de seguridad de la información, estableciendo un nexo con aquellos funcionarios que cumplen igual función en otros servicios, comunicando incidentes de seguridad a la alta dirección. Dirige y preside el Comité de Seguridad de la Información.

Política de seguridad: Conjunto de normas o buenas prácticas, declaradas y aplicadas por la institución, cuyo objetivo es disminuir el nivel de riesgo en la realización de un conjunto de actividades de interés de la organización.

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Riesgo: Probabilidad de ocurrencia de un evento inesperado, que afecte el normal funcionamiento de la institución.

4. RESPONSABILIDADES

Comité de Seguridad de la Información (CSI): Es responsable ante la Dirección Nacional por la existencia y cumplimiento de las medidas de seguridad de la información acorde con las necesidades de IPS, los recursos disponibles y normativa vigente. Aprueba políticas, protocolos y temas referentes a la seguridad de la información.

Departamento de Seguridad de la Información (DSI): Es el encargado de gestionar y controlar el sistema de seguridad de la información, sobre los activos de información del instituto, conforme a la normativa vigente y los objetivos estratégicos institucionales. Es quien informa al Comité de Seguridad de la Información y al/ la funcionario/a Encargado/a de Seguridad de la Información, la evaluación del daño de un incidente. Asimismo es responsable de rescatar y asegurar el equipamiento que se mantenga útil, evaluar los daños y planificar la recuperación del sitio del desastre.

Dirección Nacional: Tiene como responsabilidad aprobar las estrategias y mecanismos de control para el tratamiento de riesgos que afecten a los activos de información institucionales y la continuidad de las operaciones.

DIVISIÓN JURÍDICA V°B° DEPTO. CONTROL JURÍDICO I.P.S.

Encargado de Seguridad de la Información (ESI): Es el representante del Director Nacional en la definición y aplicación de los criterios de seguridad de la información en IPS. Es responsable de velar por el fiel cumplimiento de las politicas de seguridad, sus normas y procedimientos. Asimismo debe asesorar al DN en materia de seguridad de la información, y debe dirigir el CSI.

División Jurídica: Su función es dirigir, gestionar, coordinar, evaluar y controlar la función jurídica institucional, asegurando que esta sea un apoyo trasversal, eficiente, eficaz y oportuno para la gestión del Instituto, debiendo asesorar a la Dirección Nacional, Direcciones Regionales, y a las unidades del Instituto para que la toma de decisiones y la ejecución de sus labores sean conformes a derecho. Debe realizar el control de legalidad preventivo y ex post en su caso, de los actos administrativos, y ejercer la representación judicial de los intereses institucionales, sea en calidad de parte o tercero cualquiera sea la materia de que se trate, ya sea, civil, laboral, administrativa, etc.

5. POLÍTICA

5.1. Establecer responsabilidades y procedimientos formales ordenados, para el reporte explicativo, respuesta eficaz y análisis posterior de los incidentes de seguridad de la información. Estos procedimientos a su vez deben detectar, monitorear, analizar e informan la posibilidad de nuevos eventos o incidentes de seguridad de la información.

5.2. Estos incidentes que afectan la seguridad de la información, deben ser comunicados de inmediato a la mesa de ayuda, la que posteriormente informará al Encargado/a de Seguridad de la Información y a los jefes respectivos según indique el procedimiento vigente, utilizando los canales apropiados, para que se tomen las medidas correspondientes y se produzca escalamiento cuando corresponda.

5.3. Todo funcionario del IPS es responsable de informar o reportar de inmediato cualquier incidente o evento que implique riesgo de pérdida de un activo de información en cuanto a su integridad, disponibilidad, confidencialidad; o de un proceso relacionado a estos activos, considerando para ello, las prioridades de la institución.

5.4. Los eventos denunciados se deben evaluar y decidir si serán clasificados o no como incidentes de seguridad de la información. Al realizar esta clasificación, se deberá determinar debilidades de los sistemas de información para la retroalimentación de los procesos, establecer acciones correctivas y medidas de mitigación futuras.

5.5. Toda persona que trabaje en la operación de sistemas deberá poseer documentación y estar capacitado en los procedimientos que se determinen, sobre cómo debe ser manejada la seguridad de la información cuando ocurre un incidente.

5.6. Se debe definir los responsables del manejo de los incidentes en los sistemas de información. A ellos, cada jefatura, les debe conceder la autoridad para llevar a cabo esta labor.

DIVISIÓN JURÍDICA V°B° DEPTO. CONTROL JURÍDICO I.P.S.

5.7. El DSI debe enviar reportes periódicos de incidentes de seguridad al Encargado de Seguridad de la Información, para que se pongan en conocimiento del CSI, de acuerdo a un calendario que establecerá ése funcionario.

5.8. El DSI debe implementar mecanismos para posibilitar que los tipos, volúmenes y costos de los incidentes de seguridad de la información sean cuantificados por el Comité de Seguridad de la Información.

5.9. Luego de que se genere un incidente de seguridad de la información, deberá realizarse una acción de seguimiento, ya sea respecto de una persona, organización o cualquier tercero que se considere responsable. Dicha acción de seguimiento podrá involucrar acciones legales (ya sea civiles, penales o administrativas), para cuyos efectos la evidencia se debe reunir, retener y presentar de forma tal de cumplir con las reglas para las evidencias establecidas en la jurisdicción pertinente.

5.10. Para los efectos del punto precedente, el DSI debe establecer un procedimiento para administrar evidencia forense de estos incidentes.

6. DIFUSIÓN

Esta política de Gestión de Incidentes de Seguridad de la Información, y sus procedimientos relacionados, como también las resoluciones, oficios y/o circulares que emanen de la Dirección Nacional o del/a Encargado/a de Seguridad de la Información, se publicarán en la página de la intranet del Instituto, y distintos medios de difusión que posee IPS, para que todo funcionario/a del IPS conozca la presente política.

7. REEVALUACIÓN

La Política de Gestión de Incidentes de Seguridad de la Información, así como sus procedimientos relacionados, serán examinados, revisados y reevaluados por el Comité de Seguridad de la Información, cada tres (3) años y extraordinariamente cuando ocurra un incidente de seguridad que afecte a un activo de información catalogado con riesgo medio y/o alto, de manera tal de introducir las modificaciones apropiadas.

DIVISIÓN JURÍDICA V°B° DEPTO. CONTROL JURÍDICO I.P.S.