APRUEBA PARA EL INSTITUTO DE PREVISIÓN SOCIAL EL DOCUMENTO DENOMINADO "POLÍTICA DE RELACIONES CON EL PROVEEDOR CÓDIGO: POL-04", EN RELACIÓN A LA SEGURIDAD DE LA INFORMACIÓN DE LA INSTITUCIÓN.

RESOLUCIÓN EXENTA Nº 635

SANTIAGO, 22 DIC 2017

V I S T O S:

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.- La Ley N° 19.886, que fija las Bases sobre Contratos Administrativos de Suministros y Prestación de Servicios, reglamentada por el D.S. Nº 250, de 2004, del Ministerio de Hacienda.

7.- El D.F.L. N° 278, de 1960, del Ministerio de Hacienda; el D.L. Nº 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 57º, de la Ley Nº 20.255.

C O N S I D E R A N D O:

1.- Que, por Resolución Exenta N° 175, de 28 de marzo de 2017, de esta Dirección Nacional se aprobó para el Instituto de Previsión Social, el nuevo documento "Política General de Seguridad de la Información Código: POL-00", cuyo objetivo es la protección de la confidencialidad, integridad y disponibilidad de la información del Instituto, por parte de sus usuarios y clientes, en concordancia con las definiciones estratégicas y a la normativa vigente.

2.- Que, a través de Resolución Exenta N° 292, de 21 de junio de 2017, esta Dirección Nacional aprobó el documento "Alcance del Sistema de Gestión de la Seguridad de la Información (SGSI) CÓDIGO:SGSI-00", cuyo objetivo es definir los límites y la aplicabilidad del Sistema de Gestión de la Seguridad de la Información en el Instituto de Previsión Social.

3.- Que, mediante Resolución Exenta N° 385, de 10 de agosto de 2017, esta Dirección Nacional aprobó el documento "Política de la Organización de la Seguridad de la Información (SGSI) Código: SGSI-02", cuyo objetivo es generar un marco de trabajo de la dirección para establecer, implementar, verificar y mejorar el desempeño de la seguridad de la información al interior de la organización.

4.- Que, por Resolución Exenta N° 558, de 09 de noviembre de 2017, esta Dirección Nacional aprobó el documento "Política de Gestión de Incidentes de Seguridad de la Información", cuyos objetivos son: a) Asegurar un enfoque consistente y eficaz sobre la gestión de los incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y su vulnerabilidad y b) Establecer acciones de mejora a partir de incidentes de seguridad para evitar su recurrencia en el futuro.

5.- Que, en el contexto indicado, la Encargada de Seguridad de la Información, ha propuesto el texto denominado **Política Relaciones con el Proveedor Código: Pol-04",** cuyo proyecto ha sido revisado por el Jefe de la División Informática y aprobado por el Presidente del Comité de Seguridad de la Información.

6.- Que, por Oficio Ordinario N°47311/2560-2017, modificado por Oficio Ordinario N°47311/2777-2017, de 02 y 30 de noviembre de 2017, respectivamente, la División Jurídica de este Instituto, aprueba y visa en cada una de sus páginas el proyecto denominado **"Política Relaciones con el Proveedor Código: Pol-04"**, la que por su materia, se encuentra exenta del trámite de Toma de Razón por parte de la Contraloría General de la República, en los términos de la Resolución N°1.600, de 2008, de ese organismo contralor.

R E S U E L V O:

1.- Apruébase, para el Instituto de Previsión Social la **"Política Relaciones con el Proveedor Código: Pol-04"**, en relación a la 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 30 de noviembre de 2017, cuyo objetivo es establecer el marco normativo para la contratación de servicios externos, en relación a la seguridad de la información para los proveedores del Instituto de Previsión Social, para todo el personal externo que trabaja para el IPS, y que en el desarrollo de sus funciones pueda tener acceso a la información, sistemas de información o recursos IPS en general, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información y sistemas manejados por el Instituto de Previsión Social.

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

3.- Cúmplase con lo dispuesto en el artículo 48°, de la Ley N°19.880, citada en Vistos N°3 y en el Instructivo Presidencial Gab. Pres. N°008, de 04 de diciembre de 2006, complementado por Circular Conjunta N°3, de 05 de enero de 2007, del Ministerio del Interior y Ministerio de Hacienda, en orden a publicar el extracto del presente acto administrativo en el Diario Oficial y texto completo del mismo en el Banner "Gobierno Transparente", por interesar a un número indeterminado de personas.

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

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 CAPRI de su dependencia
- Unidad Apoyo Documental de la División Jurídica
- A la Encargada de Seguridad del IPS

MEES/RLO/YGF/VCG/MYEW/NGR/MEGA/MRC/mrc
Aprueba "Política Relaciones con el Proveedor Código: Pol-04"

X- (Folio DTD-3575-61-24)

POLÍTICA RELACIONES CON EL PROVEEDOR

CODIGO: POL - 04

Elaborado por:	Revisado por:	Aprobado por:
Encargada de Seguridad de la Información	Jefe División Informática	Jefe División Jurídica Director Nacional Presidente Comité 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
16/08/2017	01	Todas	Todas	Versión inicial

NOTA DE ENFOQUE DE GÉNERO

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.

NOTA DE CONFIDENCIALIDAD

La información contenida en este documento es de propiedad del Instituto de Previsión Social (IPS) y debe ser tratada de acuerdo a su nivel de confidencialidad, sobre la base de las instrucciones establecidas en la política de clasificación y manejo de información. El uso no autorizado de la información contenida en este documento podrá ser sancionado de conformidad con la ley chilena. Si usted ha recibido este documento por error, le pedimos eliminarlo y avisar inmediatamente al Instituto de Previsión Social.

División Jurídica VºBº DEPTO. CONTROL JURÍDICO I.P.S.

ÍNDICE

1 OBJETIVO ____ 4

2 ALCANCE ____ 4

3 DOCUMENTOS DE REFERENCIA ____ 4

4 DEFINICIONES ____ 5

5 RESPONSABILIDADES ____ 7

6 POLÍTICA ____ 8

6.1 ACUERDOS DE SEGURIDAD EN CONTRATO CON TERCEROS ... 9

6.2 CONTRATO CON CLAUSULA (NDA) INCORPORADA ... 9

6.3 MONITOREO Y REVISIÓN DE LOS SERVICIOS DEL PROVEEDOR ... 9

7 DIFUSIÓN ____ 10

8 REEVALUACIÓN ____ 10

VºBº DEPTO. CONTROL JURIDICO I.P.S.

1 OBJETIVO

Establecer el marco normativo para la contratación de servicios externos, en relación a la seguridad de la información para los proveedores del Instituto de Previsión Social, para todo el personal externo que trabaja para el IPS y que en el desarrollo de sus funciones pueda tener acceso a la información, sistemas de información o recursos de IPS en general, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información y sistemas manejados por IPS

2 ALCANCE

Estas directrices se aplican a todos quienes cumplen funciones para el Instituto de Previsión Social (IPS), sea en sus instalaciones o fuera de ellas, pertenecientes a cualquier estamento y calidad jurídica (planta, contrata, honorarios, asesores, consultores, alumnos en práctica) así como también a personas naturales y jurídicas externas, públicas o privadas que le presten servicios.

El ámbito de control de esta política son todos los activos de información del IPS y aquellos bajo su responsabilidad. Su cobertura se extiende a la información impresa y también a aquella almacenada electrónicamente, y transmitida por cualquier soporte o medio. Se debe precisar que el presente alcance descrito en los párrafos anteriores, está circunscrito y detallado en el documento "SGSI-00 ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)".

3 DOCUMENTOS DE REFERENCIA

- Política General de Seguridad de la Información del IPS, Res. Exenta N° 175 del 28/03/2017.
- Estructura orgánica Interna de la División Informática Res. Exenta N° 610 del 9/11/2015.
- Norma ISO NCh-ISO 27001: 2013.
- Estatuto Administrativo, Ley 18.834
- Ley 19.628 Protección de datos de carácter personal.
- Ley de Compras Públicas Nº 19.886, Ley de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios.

DIVISIÓN JURÍDICA VºBº DEPTO. CONTROL JURÍDICO I.P.S.

4 DEFINICIONES

Para los propósitos de esta Política, se definen los siguientes conceptos:

a. **Activo de Información**: Elementos para la producción, procesamiento, emisión, almacenaje, comunicación, visualización y la recuperación de la información que posee valor para la organización. Pueden clasificarse en personas, infraestructura, sistemas y datos.

b. **Buen Uso de la información:** Cuidado que los colaboradores de la Institución deben procurar en el manejo o utilización de los sistemas y activos de información de la Institución, refiérase al cuidado que los usuarios deben tener en relación a los activos de información.

c. **Confidencialidad:** Propiedad de la información que consiste en que ésta no sea puesta a disposición o sea revelada a individuos, entidades o procesos no autorizados

d. **Custodio de la información:** Es el funcionario que mantiene bajo su responsabilidad información de la que no es propietario, pero que por su función es el responsable de aplicar las medidas de seguridad necesarias que se definan, de acuerdo al valor de los activos a su cargo.

e. **Documento electrónico**: Toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.

f. **Disponibilidad:** Propiedad de la información que consiste en que ésta deba estar accesible y utilizable cuando lo requiera una entidad autorizada.

g. **Evento de Seguridad de la Información:** Acontecimiento que amenaza la seguridad de la información, sin presentar resultados negativos.

h. **Incidente de seguridad de la información**: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

i. **Integridad:** La propiedad de proteger la exactitud y completitud de los activos.

j. **NDA:** Acuerdo o contrato de confidencialidad (non-disclosure agreement), es un contrato legal entre al menos dos entidades para compartir material confidencial o conocimiento para ciertos propósitos, restringiendo su uso público.

VºBº DEPTO. CONTRO JURÍDICO I.P.S.

k. **Propietario de la información:** Es quien genera, mantiene y utiliza la información, siendo responsable de ella y de los procesos que se llevan a cabo en su procesamiento, a través de diversos medios, sean éstos manuales, mecánicos o electrónicos.

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

m. **Jefatura:** Funcionario encargado de un grupo de personas, conformados en, dirección, subdirección, división, departamento o área que lo amerite definida en la estructura organizativa del instituto.

n. **Tercero:** Empresa o persona externa que tiene algún tipo de relación con la Institución.

o. **Administración de Contrato:** Planificar, dirigir, controlar, y coordinar de acuerdo a políticas, normas e instrucciones internas, legislación vigente, y términos del respectivo contrato y demás antecedentes que componen el estatuto jurídico de la contratación, todas las actividades orientadas a obtener el producto o servicio materia del contrato, en la oportunidad y calidad requerida para atender las necesidades de operación o gestión del IPS. Junto con ello, velar por el fiel cumplimiento de las obligaciones contractuales, tanto las del IPS para con el proveedor o empresa contratada, cómo de ésta para con el IPS, informar a su jefatura de los incumplimientos y proponer las respectivas sanciones que correspondiere, conforme a lo estipulado en el contrato.

p. **Administrador del contrato o la Relación Contractual:** funcionario de planta o contrata, designado por Resolución en calidad de titular o suplente, quien en nombre y representación del IPS -facultado por éste- se relaciona con la empresa contratada y cumple la función de administrar el contrato y velar por el fiel, oportuno y correcto cumplimiento del mismo.

q. **Contrato:** acto jurídico bilateral, que genera derechos y obligaciones para las partes. El Instituto tiene el derecho de exigir al tercero contratado una determinada prestación de servicios, o entrega del bien o producto, que espera recibir dentro de plazo, en la forma y calidad solicitada, a cambio de ello, tiene la obligación de pagar oportunamente la prestación de servicios, bien o producto contratado. Todo ello, conforme a la normativa vigente, las bases de la licitación, o términos de referencia correspondientes, y la oferta aceptada o adjudicada que presentó el tercero. El derecho de una de las partes constituye la obligación de la otra parte contratante.

División Jurídica VºBº DEPTO. CONTROL JURÍDICO I.P.S.

5 RESPONSABILIDADES

a) **Encargado de la Seguridad de la Información (ESI):** Funcionario que publica, difunde y supervisa el cumplimiento de las políticas de seguridad de la información, establece nexo con sus pares en la materia, que pertenezcan a otros servicios, y comunica la eventual ocurrencia de incidentes de seguridad al Comité de Seguridad de la Información. Dirige y preside el Comité de Seguridad de la Información.

b) **División Jurídica**: Revisa las cláusulas de Seguridad de la información en los contratos celebrados por la División Informática, con sus proveedores de servicio.

c) **Administrador de contrato**: Encargado de planificar, dirigir, controlar, y coordinar de acuerdo a políticas, normas e instrucciones internas, legislación vigente, y términos del respectivo contrato y demás antecedentes que componen el estatuto jurídico de la contratación, todas las actividades orientadas a obtener el producto o servicio materia del contrato, en la oportunidad y calidad requerida para atender las necesidades de operación o gestión del IPS. Junto con ello, velar por el fiel cumplimiento de las obligaciones contractuales, tanto las del IPS para con el proveedor o empresa contratada, cómo de ésta para con el IPS, informar a su jefatura de los incumplimientos y proponer las respectivas sanciones que correspondiere, conforme a lo estipulado en el contrato.

d) **Departamento de Administración e Inmobiliaria:** Encargado de supervisar los contratos menores a 1.000 UTM establecidos por su competencia.

e) **Comité de Seguridad de la Información (CSI):** Es un comité 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 la normativa vigente.

f) **Jefe División de Informática (DI):** Es el responsable del diseño, implementación y mantención tecnológica de las necesidades institucionales en materias de seguridad de la información, como de velar por la administración de los contratos frente a los proveedores de esta división.

VºBº DEPTO. CONTROL JURÍDICO IPS

6 POLÍTICA

a) Si un tercero efectúa una tarea para IPS, debe ceñirse a lo establecido en el documento Procedimientos para la Administración de Contratos, numeral 6, denominado Procedimientos; y Elaboración de Bases Administrativas y Técnicas.

b) Los servicios de terceros deben ampararse por un contrato, firmado por la Dirección Nacional o por la autoridad responsable para ello, el cual debe ser previamente revisado y validado por el área jurídica de la repartición, como lo establece la ley.

c) El contrato debe incluir el fiel y oportuno cumplimiento de las obligaciones laborales y previsionales de los trabajadores.

d) Al otorgar acceso a información a terceros, el Departamento de Seguridad de Información de la División Informática, el Encargado de Seguridad de la Información y el Propietario de la Información de que se trate, analizarán el riesgo de ello, teniendo en cuenta:

- El tipo de acceso requerido (físico/lógico y a qué recurso).
- Los motivos por los cuales se solicita el acceso.
- El valor de la información.
- Los controles empleados por la tercera parte.
- La incidencia de este acceso en la seguridad de la información.
- Ley 19.628 Protección de datos de carácter personal.

e) Para las prestaciones de servicio que se desarrollen dentro de IPS, se establece los controles, requerimientos de seguridad y compromisos de confidencialidad, restringiendo según necesidad del servicio su acceso.

f) No se debe otorgar acceso a terceros a la información, en las instalaciones de procesamiento u otras áreas de servicios críticos. Esto es implementado usando los controles apropiados y se firma un contrato o acuerdo que defina las condiciones para el mencionado acceso, basado en lo establecido en la Política de Seguridad Física y del Ambiente.

VºBº DEPTO. CONTROL JURÍDICO IPS

6.1 ACUERDOS DE SEGURIDAD EN CONTRATO CON TERCEROS

Los contratos o acuerdos existentes, con terceros deben contemplar:

a) Cumplimiento de la Política General de Seguridad de la Información del Instituto de Previsión Social.
b) Protección de los activos de información, considerando:

- Procedimiento de Inventario de Activos de Información; para proteger los activos de información.
- Restricciones a la copia y divulgación de información.

c) Acuerdos de control de acceso, autorizados por el Departamento de Seguridad de Información de la División Informática, considerando:

- Política de Control de acceso a la información física y digital.
- Autorización de accesos y privilegios de usuarios.
- Mantención actualizada de una lista de individuos autorizados a utilizar los servicios, con sus derechos y privilegios respecto al uso.
- Definición de controles que garanticen la protección contra software malicioso.

6.2 CONTRATO CON CLAUSULA (NDA) INCORPORADA

a) El contrato debe contener una cláusula de confidencialidad, restringiendo el uso de la información a los fines específicos de la institución, protegiendo el negocio, según lo establecido en la Resolución Exenta N° 20 del 25/01/2016 modificada por la Resolución Exenta N°118 del 18/03/2016, denominada "Instrucción de Trabajo para Administración de Contrato".

b) Todo contrato debe basarse en la Ley de Compras Públicas Nº 19.886, Ley de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios.

c) Ley 19.628 Protección de datos de carácter personal.

6.3 MONITOREO Y REVISIÓN DE LOS SERVICIOS DEL PROVEEDOR

a) Se debe monitorear, revisar y auditar los servicios del proveedor de manera regular.

DIVISION JURIDICA V°B° DEPTO. GENERAL JEFES I.P.S.

b) Se debe mantener registros de revisión de los servicios de proveedores externos (actas de reunión, mail, revisiones del contrato) para los Operadores de Comunicaciones, Proveedor de Wireless y Facturación Online, entre otros.

7 DIFUSIÓN

La política, sus normas y procedimientos, y sus correspondientes actualizaciones y/o modificaciones, así como también las resoluciones, oficios y/o circulares que emanen de la Dirección Nacional o del Encargado de Seguridad de la Información, deben publicarse en la página de la intranet del IPS.

Se debe generar e implementar un Plan de Comunicación y Sensibilización de esta política, además de otras acciones de comunicación y difusión por los distintos medios que posee el IPS.

8 REEVALUACIÓN

La política será examinada, revisada y reevaluada cada año, y extraordinariamente, cuando se produzcan cambios en el enfoque a la gestión de seguridad, que generen cambios en las circunstancias de la institución, debido a cambios legales, en el ambiente técnico o bien las recomendaciones realizadas por las autoridades competentes así lo aconsejen. Asimismo deberá reevaluarse esta política cuando existan amenazas a la información o se detecten vulnerabilidades en los sistemas, de tal manera que hagan aconsejables una revisión de la misma.