Por motivo de la MEI de Seguridad de la Información 2013, se hace necesario realizar una actualización del Protocolo de Manejo responsable de Información de forma que aborde los conceptos asociados a la MEI antes indicada.

Se adjunta el texto del Protocolo con las sugerencias y comentarios para su consideración.

Superintendencia de Pensiones

"Protocolo de Manejo Responsable de Información"

Superintendencia de Pensiones

Noviembre 2013

Índice

1 Introducción

La Superintendencia de Pensiones (SP), en su rol de regulador y supervisor del sistema previsional, tanto del pilar solidario como contributivo y del seguro de cesantía, recibe, elabora y solicita información clave para el desarrollo de sus funciones. Asimismo, la información se utiliza para la difusión de aspectos de interés público relacionados al funcionamiento y desempeño del sistema previsional chileno, así como para la elaboración de reportes y análisis desarrollados a nivel interno de la SP.

El manejo de esta información es un aspecto de gran relevancia para la Superintendencia de Pensiones ya que una parte sustantiva de esta información es de alta sensibilidad y está protegida por ley, transformándose en un deber para la propia SP, sus funcionarios y para sus regulados, el manejo responsable de dicha información. En la medida que las normas de seguridad y manejo de información estén claramente establecidas y sean conocidas por todos los funcionarios de la SP, menor es la probabilidad de infringir las obligaciones estipuladas en la ley y mayor es el grado de protección de la información de los afiliados y de los propios funcionarios que utilizan información sensible.

El presente Protocolo de Manejo Responsable de Información es una herramienta que precisamente contribuye a aumentar el grado de seguridad de la información que se maneja en la SP y a elevar el nivel de capacitación del personal en cuanto a una mejor comprensión de las responsabilidades involucradas. Cabe destacar que este protocolo no pretende ser un manual de proceso respecto del manejo de información ni de la seguridad informática de la institución, sino una guía orientadora para el manejo habitual de información, quedando a la responsabilidad personal, la iniciativa para canalizar oportunamente en los superiores respectivos, las situaciones que no estuvieran contempladas en este documento. La información sujeta al protocolo abarca tanto la información que se genera y maneja en la propia SP como aquella que se intercambia con las instituciones reguladas y con otros organismos y personas que tienen relación con la SP.

La sección 2 de este documento entrega una revisión de las principales disposiciones regulatorias que dan cuenta de las atribuciones y responsabilidades, tanto institucionales como personales, derivadas del uso de información, la sección 3 describe el marco general de administración y uso de la información en la SP, la sección 4 entrega las bases para el intercambio de información con otras instituciones o personas y la sección 5 detalla los resguardos a considerar cuando externos puedan tener acceso a información en la SP.

El Protocolo de Manejo Responsable de Información es un documento elaborado y sancionado por el Comité de Planificación de la Superintendencia de Pensiones, instancia encargada de generar las directrices en esta materia y resolver las consultas que emanen de su utilización. Una de las labores de este comité es recoger las sugerencias y recomendaciones para el continuo perfeccionamiento de este documento.

2 Marco Regulatorio para el Manejo Responsable de Información

En esta sección se presenta un resumen de las principales disposiciones legales y reglamentarias relacionadas con el manejo y acceso a información vinculada a las labores habituales de la SP. Con este documento se espera generar conocimiento en el personal de la Superintendencia acerca de las responsabilidades que emanan del acceso a información de carácter reservado.

Las sanciones asociadas a la infracción de las disposiciones legales y normativas citadas en esta sección dependerán de las circunstancias y características propias de cada caso.

Con el objetivo de difundir e incrementar el conocimiento respecto del "Protocolo de Manejo Responsable de Información", una vez al año la SP realizará una capacitación de este tópico a nivel institucional, la cual deberá formar parte del programa de capacitación estratégica de la Superintendencia y del programa de inducción para funcionarios nuevos. Los jefes de las divisiones y unidades informarán al Comité de Planificación (CP) sobre los participantes en esta actividad y será el CP que aprobará en cada oportunidad, el contenido y el énfasis de esta actividad de capacitación.

Por otra parte, será obligación de la Unidad de Auditoría Interna de la SP, auditar a lo menos a una Unidad o Departamento, como parte de su programa anual de actividades. La auditoría deberá tener como objetivo principal reportar el grado de cumplimiento e implementación de los procedimientos contenidos en el presente protocolo. Las conclusiones y hallazgos derivados de las auditorías deberán ser reportadas al Comité de Planificación, debiendo este último, determinar las acciones que corresponda para corregir potenciales anomalías y elaborar un plan de mitigación de los riesgos identificados.

Las disposiciones regulatorias que se presentan en esta sección se ordenan partiendo por aquellas que tienen rango legal y luego normativas. La revisión se inicia con los artículos de leyes que se relacionan con el ámbito de fiscalización de la Superintendencia de Pensiones, es decir, las del sistema previsional (DL N° 3.500 y Ley 20.255) y del Seguro de Cesantía (Ley N° 19.728), luego se presentan las disposiciones legales vinculadas a la protección de información que son de aplicación más general y por último, las regulaciones legales que norman el intercambio y entrega de información por parte de instituciones públicas. En el ámbito normativo se mencionan específicamente los artículos relacionados a la información confidencial contenidos en el "Código de Ética de la SP". No obstante la revisión legal y normativa incluida en este documento, los funcionarios deberán tener en cuenta la normativa general que rige el actuar de los funcionarios públicos, en particular la Ley N° 19.653 sobre probidad administrativa aplicable a los órganos de la administración del Estado.

2.1 Disposiciones Legales del Sistema Previsional y del Seguro de Cesantía

El artículo 50 de la Ley 20.255 señala/[1]:

> *"Artículo 50.- La Superintendencia de Pensiones podrá requerir datos personales y la información que fuere necesaria para el ejercicio de sus funciones a instituciones públicas y a organismos privados del ámbito previsional o que paguen pensiones de cualquier tipo. Con todo, en el caso de los organismos privados la información que se requerirá deberá estar asociada al ámbito previsional. Además, podrá realizar el tratamiento de los datos personales con el fin de ejercer el control y fiscalización en las materias de su competencia.*
>
> *Para estos efectos, no regirá lo establecido en el inciso segundo del artículo 35 del Código Tributario.*
>
> *El Superintendente y todo el personal de la Superintendencia deberán guardar reserva y secreto absolutos de las informaciones de las cuales tomen conocimiento en el cumplimiento de sus labores. Asimismo, deberán abstenerse de usar dicha información en beneficio propio o de terceros. Para efectos de lo dispuesto en el inciso segundo del artículo 125 de la ley N° 18.834, cuyo texto refundido, coordinado y sistematizado fue fijado por el decreto con fuerza de ley N° 29, de 2005, del Ministerio de Hacienda, se estimará que los hechos que configuren infracciones a esta disposición vulneran gravemente el principio de probidad administrativa, sin perjuicio de las demás sanciones y responsabilidades que procedan".*

El DL 3.500 también impone resguardos especiales a la información en determinadas circunstancias. Así, respecto del proceso de Consulta en SCOMP y del tratamiento de la información en este proceso, se señala en los incisos 11° y 12° del artículo 61 bis:

> *Artículo 61 bis.- Las Administradoras de Fondos de Pensiones, las Compañías de Seguros de Vida y los asesores previsionales que participen en el Sistema de Consultas y Ofertas de Montos de Pensión, serán responsables de la transmisión íntegra de la información de dicho Sistema. Asimismo, deberán resguardar la privacidad de la información que manejen de acuerdo a lo dispuesto en la ley N° 19.628, sobre protección de datos de carácter personal, y quedarán sujetas a las responsabilidades que en dicha ley se establecen.*
>
> *El que obtenga beneficio patrimonial ilícito mediante fraude al afiliado o a sus beneficiarios o el que haga uso no autorizado de los datos de éstos, que en virtud de este artículo deban proporcionarse al Sistema o de aquellos contenidos en el listado a que se refiere el artículo 72 bis, será sancionado con las penas establecidas en el artículo 467 del Código Penal, sin perjuicio de las demás sanciones legales o administrativas que correspondan.*

/[1] La Ley 20.255 que contiene la Reforma Previsional publicada en el D.O. el 17 marzo de 2008.

En relación a la información de las carteras de inversiones de los Fondos de Pensiones, el D.L. 3.500, establece el umbral para que dicha información pueda ser de conocimiento público. A partir de esta disposición y la normativa complementaria de la SP relativa a la información de cartera de los Fondos de Pensiones se establece que la información pública se circunscribe a aquella que la SP tiene disponible en su sitio web y toda otra información o estadística relativa a los Fondos o Administradoras es confidencial.

> *Artículo 26.- Toda publicación de la composición de la cartera de inversión de los distintos Tipos de Fondos de Pensiones de cada una de las Administradoras, deberá referirse a períodos anteriores al último día del cuarto mes precedente. El contenido de dichas publicaciones se sujetará a lo que establezca una norma de carácter general de la Superintendencia. Con todo, esta última podrá publicar la composición de la cartera de inversión agregada de los Fondos de Pensiones referida a períodos posteriores al señalado.*

Asimismo, se debe tener en consideración las siguientes disposiciones del DL 3.500, las cuales afectan principalmente a los funcionarios que apoyen las labores de un inspector delegado, miembros de la SP que participan en la Comisión Clasificadora de Riesgo (CCR) y en el Consejo Técnico de Inversiones (CTI).

> *Artículo 94.- En el ejercicio de sus funciones, el inspector podrá hacerse acompañar por otros funcionarios de la Superintendencia, así como contratar consultorías privadas externas con cargo a la Administradora. Tanto el inspector delegado como dichos funcionarios deberán guardar absoluta reserva y secreto de la información de las cuales tomen conocimiento en el cumplimiento de sus labores y deberán abstenerse de usar dicha información en beneficio propio o de terceros. Para efectos de lo dispuesto en el inciso 2° del artículo 125 del decreto con fuerza de ley N° 29 de 2004 del Ministerio de Hacienda, se estimará que los hechos que configuren infracciones a lo dispuesto en esta norma vulneran gravemente el principio de probidad administrativa, lo que no obstará a las demás responsabilidades y sanciones que fueren procedentes*

> *Artículo 103.- Los integrantes de la Comisión Clasificadora, como también los funcionarios públicos deberán guardar reserva sobre los documentos y antecedentes de los emisores e instrumentos sujetos a clasificación, siempre que éstos no tengan carácter público. La infracción a esta obligación será sancionada con la pena de reclusión menor en su grado mínimo a medio.*
>
> *Del mismo modo, les está prohibido valerse, directa o indirectamente, en beneficio propio o de terceros, de la información a que tengan acceso en el desempeño de esta función, durante el lapso que dure la reserva establecida en el inciso primero del artículo 109 será sancionada con la pena de reclusión menor en su grado medio e inhabilitación para cargos y oficios públicos por el tiempo de la condena.*
>
> *Los miembros de la Comisión Clasificadora, los integrantes de la Secretaría Administrativa, los funcionarios públicos o aquellas personas que tomen conocimiento de las proposiciones de aprobación de instrumentos o de las clasificaciones presentadas a la Comisión Clasificadora para su consideración, que presentaren o difundieren información falsa o tendenciosa respecto de los instrumentos que aquella deba aprobar o rechazar, sufrirán la pena de reclusión menor en sus grados mínimo a medio e inhabilitación para ejercer cargos en la Comisión Clasificadora y en cualquier oficio público por todo el tiempo que dure la condena, sin perjuicio de las acciones civiles que correspondan.*

Artículo 168 (incisos 8 y 9). - Los miembros titulares y suplentes y el Secretario Técnico del Consejo deberán guardar reserva sobre los documentos y antecedentes a que tengan acceso en el ejercicio de su función, siempre que éstos no tengan carácter público. La infracción a esta obligación será sancionada con la pena de reclusión menor en sus grados mínimo a medio.

Del mismo modo, a las personas indicadas en el inciso precedente les está prohibido valerse, directa o indirectamente, en beneficio propio o de terceros, de la información a que tengan acceso en el desempeño de esta función, en tanto no sea divulgada al público. La infracción a lo dispuesto en este inciso será sancionada con la pena de reclusión menor en su grado medio e inhabilitación para cargos y oficios públicos por el tiempo de la condena.

En el contexto de la Ley 19.728 que establece el Seguro de Cesantía, el artículo 34 A, establece la protección a la Base de Datos de afiliados al Seguro de Cesantía.

Artículo 34 A: "Para el desarrollo de estudios de carácter técnico del artículo, la Superintendencia podrá requerir la información de la Base de Datos a que se refiere dicho artículo que fuere necesaria para el cumplimiento de los objetivos establecidos en él y con el fin de ejercer el control y fiscalización en las materias de su competencia, pudiendo realizar el tratamiento de datos personales que esta Base contenga.

El personal de la Superintendencia deberá guardar absoluta reserva y secreto de las informaciones de las cuales tome conocimiento en el cumplimiento de sus funciones sin perjuicio de las informaciones y certificaciones que deba proporcionar de conformidad a la ley.

2.2 Disposiciones Legales de Aplicación General

La Ley N° 19.628/[2] se refiere al tratamiento de los datos personales con el fin de proteger la identidad e integridad de las personas contenidas en las bases de datos. Adicionalmente, dicha ley faculta a las instituciones públicas a utilizar las bases de datos para cumplir con sus funciones. En sus artículos 7, 11 y 20 indica lo siguiente:

Artículo 7.- Las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo.

Artículo 11.- El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños.

Artículo 20.- El tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular.

/[2] La Ley 19.628 sobre protección de datos de carácter personal promulgada el 28 de agosto de 1999.

Por su parte, la Ley N°19.223/[3] que tipifica las figuras penales relativas a la informática en sus artículos 1° al 4° indica lo siguiente:

> *"Artículo 1°.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.*
>
> *Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.*
>
> *Artículo 2°.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.*
>
> *Artículo 3°.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.*
>
> *Artículo 4°.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.".*

2.3 Disposiciones Legales para el Intercambio y Entrega de Información

La modificación legal incorporada a la Ley General de Bancos por el proyecto conocido como MKII o Ley 20.190/[4] respecto de la facultad de compartir información institucional entre las Superintendencias señala:

> *Artículo 18 bis Ley General de Bancos: "Con el objeto de velar por el cumplimiento de sus respectivos deberes de fiscalización, los Superintendentes de Bancos e Instituciones Financieras, de Valores y Seguros y de Administradoras de Fondos de Pensiones podrán compartir cualquier información, excepto aquella sujeta a secreto bancario. Cuando la información compartida sea reservada, deberá mantenerse en este carácter por quienes la reciban."*

En el mismo sentido, la norma especial contenida en el artículo 30 de la Ley N°20.403, indica:

> *"Las Subsecretarías de Hacienda y de Previsión Social y la Dirección de Presupuestos, estarán facultadas, en el ejercicio de sus funciones, para acceder a la información contenida en el Sistema de Información de Datos Previsionales a que se refiere el artículo 56 de la Ley N°20.255, y requerir los datos personales y la información asociada al ámbito previsional que posean otros organismos públicos, los que quedarán dentro del ámbito de control y fiscalización de dichos servicios.*

/[3] La Ley N° 19.223 del Ministerio de Justicia que tipifica las figuras penales relativas a la informática fue publicada el 7 de julio de 1993.

/[4] La Ley N° 20.190 o reforma al mercado de capitales II fue publicada en el D.O. en junio de 2010.

Los organismos públicos antes señalados y su personal deberán guardar absoluta reserva y secreto de la información de que tomen conocimiento y abstenerse de usar dicha información en beneficio propio o de terceros. Para efectos de lo dispuesto en el inciso 2° del artículo 125 del decreto con fuerza de ley N° 29, de 2005, del Ministerio de Hacienda, se estimará que los hechos que configuren infracciones a esta disposición vulneran gravemente el principio de probidad administrativa, sin perjuicio de las demás sanciones y responsabilidades que procedan".

La Ley N° 19.728 que establece el Seguro Obligatorio de Cesantía en su artículo 34 B señala:

Artículo 34 B.- Las Subsecretarías de Hacienda y del Trabajo y la Dirección de Presupuestos, estarán facultados para exigir los datos personales contenidos en la Base de Datos a que se refiere el artículo 34 y la información que fuere necesaria para el ejercicio de sus funciones a la Sociedad Administradora de Fondos de Cesantía. En tal caso, el tratamiento y uso de los datos personales que efectúen los organismos antes mencionados quedarán dentro del ámbito de control y fiscalización de dichos servicios.

Los organismos públicos antes señalados y su personal deberán guardar absoluta reserva y secreto de la información de que tomen conocimiento y abstenerse de usar dicha información en beneficio propio o de terceros. Para efectos de lo dispuesto en el inciso segundo del artículo 125 de la Ley N° 18.834, cuyo texto refundido, coordinado y sistematizado fue fijado por el decreto con fuerza de ley N° 29, de 2005, del Ministerio de Hacienda, se estimará que los hechos que configuren infracciones a esta disposición vulneran gravemente el principio de probidad administrativa, sin perjuicio de las demás sanciones y responsabilidades que procedan. Asimismo, le serán aplicadas las sanciones establecidas en el inciso sexto del artículo 34 de la presente ley.

Frente a las solicitudes de información que invoquen la Ley N° 20.285 sobre acceso a Información pública /[5], se deberán tener en cuenta el artículo quinto y el vigésimo primero que indican lo siguiente:

Artículo 5°: En virtud del principio de transparencia de la función pública, los actos y resoluciones de los órganos de la Administración del Estado, sus fundamentos, los documentos que les sirvan de sustento o complemento directo y esencial, y los procedimientos que se utilicen para su dictación, son públicos, salvo las excepciones que establece esta ley y las previstas en otras leyes de quórum calificado.

Asimismo, es pública la información elaborada con presupuesto público y toda otra información que obre en poder de los órganos de la Administración, cualquiera sea su formato, soporte, fecha de creación, origen, clasificación o procesamiento, a menos que esté sujeta a las excepciones señaladas.

Artículo 21: Las únicas causales de secreto o reserva en cuya virtud se podrá denegar total o parcialmente el acceso a la información, son las siguientes:

1. *Cuando su publicidad, comunicación o conocimiento afecte el debido cumplimiento de las funciones del órgano requerido, particularmente:*

[5] La Ley 20.285 sobre acceso a la información pública fue publicada en el D.O el 20 de agosto de 2008.

a) Si es en desmedro de la prevención, investigación y persecución de un crimen o simple delito o se trate de antecedentes necesarios a defensas jurídicas y judiciales.

b) Tratándose de antecedentes o deliberaciones previas a la adopción de una resolución, medida o política, sin perjuicio que los fundamentos de aquéllas sean públicos una vez que sean adoptadas.

c) Tratándose de requerimientos de carácter genérico, referidos a un elevado número de actos administrativos o sus antecedentes o cuya atención requiera distraer indebidamente a los funcionarios del cumplimiento regular de sus labores habituales.

2. *Cuando su publicidad, comunicación o conocimiento afecte los derechos de las personas, particularmente tratándose de su seguridad, su salud, la esfera de su vida privada o derechos de carácter comercial o económico.*

3. *Cuando su publicidad, comunicación o conocimiento afecte la seguridad de la Nación, particularmente si se refiere a la defensa nacional o la mantención del orden público o la seguridad pública.*

4. *Cuando su publicidad, comunicación o conocimiento afecte el interés nacional, en especial si se refieren a la salud pública o las relaciones internacionales y los intereses económicos o comerciales del país.*

5. *Cuando se trate de documentos, datos o informaciones que una ley de quórum calificado haya declarado reservados o secretos, de acuerdo a las causales señaladas en el artículo 8° de la Constitución Política.*

Respecto de la entrega de información por parte de la SP se debe tener en consideración que el legislador ha pretendido conservar la supervisión de la información traspasada en cada caso en la institución responsable de la base de datos respectiva. En efecto, al señalar el artículo 30 de la Ley 20.403 que esta facultad se confiere dentro del ámbito de su competencia, obliga al responsable de la base de datos a cerciorarse que nos encontramos en este ámbito, para permitir el acceso a la información requerida.

Por otro lado, también resulta evidente que una vez definido el acceso y la información traspasable en cada requerimiento, éste se ha otorgado con amplitud en relación a su contenido, esto es, incluyendo aquella información personalizada determinada o determinable, si ésta resultare necesaria para el ejercicio de las funciones del organismo requirente en conformidad a su solicitud. Será por tanto, necesario que el organismo solicitante señale, conjuntamente con la petición, una descripción definida y clara de la información requerida y los motivos institucionales así como los objetivos que fundamentan la generación de dicho requerimiento. En razón de la importancia y sensibilidad de la información se deberán establecer las vías de transmisión de dicha información privilegiando su seguridad.

2.4 Código de Ética de la SP

Además de los cuerpos legales antes citados, parte esencial del manejo de información está contenido en el Código de Ética de la SP. En su sección 3 sobre principios esenciales que deben regir el actuar de los funcionarios de la institución, el código señala:

> *7. Discreción. "Guardar reserva respecto de hechos o informaciones de los que tenga conocimiento con motivo o en ocasión del ejercicio de sus funciones, sin perjuicio de los deberes y las responsabilidades que le correspondan en virtud de las normas que regulan la transparencia y el acceso a la información pública. Asimismo, abstenerse de usar dicha información en beneficio propio o de terceros. En particular, debe dar estricto cumplimiento a lo dispuesto en el artículo 50 de la Ley N° 20.255"*

En la sección de prohibiciones éticas:

> *3. Hacer uso de información privilegiada. Participar o permitir que otros participen en hechos en lo que se utilice información privilegiada a la que ha tenido acceso por su condición o ejercicio del cargo que desempeña.*

En el artículo 5. "Deber de reserva y abstención de uso de información sensible con valor económico y de transacción de valores:

> *Además del deber de reserva, quienes se desempeñen en la Superintendencia estarán obligados a velar porque la información antedicha quede debidamente salvaguardada, para lo cual aquellos deberán adoptar o requerir la implementación de las medidas pertinentes para evitar que la información de que disponen pueda ser objeto de uso inadecuado.*

El artículo 6.- Deber de manejo apropiado de bases de datos

> *Las personas que se desempeñen en la Superintendencia deberán mantener en reserva la información relativa a datos personales de afiliados a las Administradoras de Fondos de Pensiones, al Instituto de Previsión Social y a la Administradora de Fondos de Cesantía. En ese sentido, deberán adoptar las medidas necesarias destinadas a proteger la información reservada de las personas contenida en las bases de datos y evitar que la información de que disponen pueda ser objeto de uso inadecuado. Para ello, deberán regirse por el manual de normas operativas que establezca la Superintendencia para el adecuado uso de los datos personales de los afiliados a las Administradoras de Fondos de Pensiones, al Instituto de Previsión Social y a la Sociedad Administradora de Fondos de Cesantía.*
>
> *En el manejo de bases de datos, todo el personal de la Superintendencia deberá sujetarse a las obligaciones y prohibiciones siguientes:*
>
> *a. Deberán guardar estricta reserva de la información de índole personal y no publica de afiliados, respecto de la cual accedan en el cumplimiento de sus labores.*

b. *No podrán usar la información de índole personal y no publica de afiliados, respecto de la cual accedan en el cumplimiento de sus labores, en beneficio propio o de terceros.*

c. *Solo podrán efectuar el tratamiento de bases de datos con información de carácter personal de afiliados, respecto de las materias de su competencia en el ejercicio de su cargo.*

d. *Solo en los casos que sea necesario para fines de fiscalización y control, podrán tener acceso a bases de datos nominadas.*

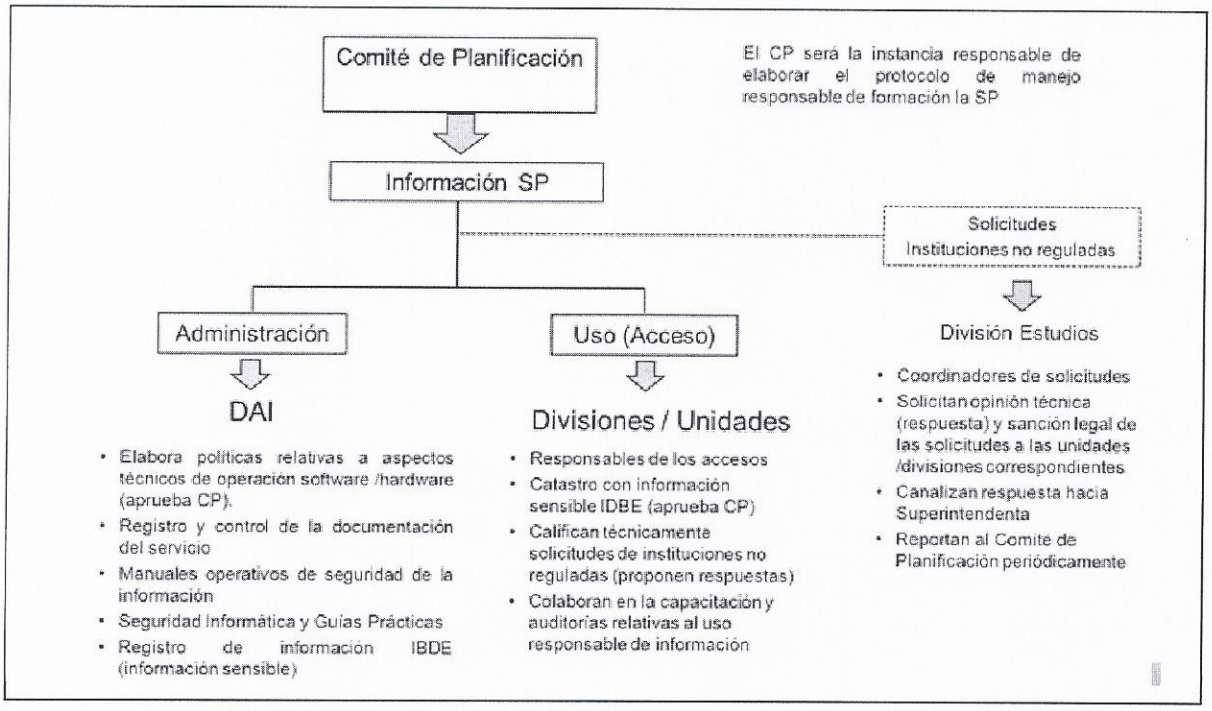
3 Administración y Uso de la Información en la SP

3.1 Funcionamiento Institucional

La instancia encargada de la elaboración del Protocolo de Manejo Responsable de la Información es el Comité de Planificación de la SP, integrado por la Superintendenta, el Fiscal, los Intendentes de Regulación y Fiscalización, el Jefe la División de Administración Interna e Informática y la Coordinadora de Gestión de la SP.

Para efectos del presente protocolo se distinguirá entre administración y uso de la información. La función de administración se refiere a los aspectos técnicos (operación / hardware / software) y de seguridad informática cuyo responsable es la División de Administración Interna e Informática (DAI), conforme a las funciones asignadas por el D.F.L. 101 de 1980 y sin perjuicio de las otras funciones asignadas a la DAI en este decreto. Para cumplir con este propósito, la DAI elaborará sus propias políticas y manuales de operación, los cuales estarán orientados a facilitar el trabajo de los funcionarios en esta área. No obstante, los cambios en las políticas estratégicas en el ámbito de la administración de la información institucional deberán ser aprobados por el Comité de Planificación de la SP. Por su parte, el uso de la información será determinado por el Comité de Planificación, instancia que autorizará y/o restringirá el acceso a la información a las Divisiones u otras unidades de la Superintendencia.

Cuadro 1
Funcionamiento Institucional



Sin perjuicio de lo anterior, el Superintendente determina que unidades o divisiones son las responsables técnicas de las bases de datos o fuentes de información. Por responsables técnicos se entiende en este contexto, aquellas unidades que gestionan la operación de las bases de datos y sus modificaciones en conjunto con la DAI.

Un rol especial en este esquema tendrá la División de Estudios que será la unidad encargada de canalizar todas las solicitudes externas de información y/o datos con personas naturales o instituciones no reguladas desde y hacia SP, debiendo realizar las consultas técnicas y jurídicas que corresponda en cada caso, generar las respuestas o solicitudes para la sanción de la Superintendenta, en base a la propuesta de las unidades especializadas y reportar al Comité de Planificación periódicamente sobre los flujos de información hacia y desde la SP con instituciones no reguladas.

3.2 Alcance del Protocolo

El alcance de este protocolo y sus recomendaciones se extienden a toda la información que existe y se maneja en la Superintendencia de Pensiones, tanto física como electrónica, datos, bases de datos, expedientes y documentación en general. No obstante, el Comité de Planificación podrá requerir que determinada información que se denominará IBDE (Información y Bases de Datos Especiales), se someta a los procedimientos especiales consignados en la sección 3.3 del presente protocolo, en razón de la necesidad de limitar su acceso o de requerir un tratamiento especial para su uso y/o almacenamiento. Ejemplos de información IBDE que será tratada bajo los resguardos definidos en la sección 3.3 es la información recabada desde las instituciones reguladas para la aplicación de las fiscalizaciones bajo el enfoque de Supervisión Basada en Riesgos (SBR), las bases de datos de Afiliados (BDA), las bases de datos del Seguro de Cesantía, las bases de datos de beneficiarios del IPS, los expedientes de sanciones, los expedientes médicos, bases de licitación en elaboración, datos relativos a la cartera de inversiones de los Fondos de Pensiones e información reservada recibida por la SP desde otras instituciones.

Las bases de datos que contengan información "nominada" deberán ser siempre clasificadas como IBDE y ser tratadas bajo el protocolo de la sección 3.3, el cual considera un estricto procedimiento de autorización, establecimiento de perfil de acceso e incorporación al Registro de Accesos IBDE. Se entenderá por bases de datos nominadas aquellas bases de datos en que es posible identificar información personalizada o individual de personas naturales o jurídicas, ya sea directamente (por ejemplo a través de rut y/o nombre) o indirectamente a través de otra información que por sí sola o combinada permita individualizar la información. Las bases de datos que en razón de su contenido confidencial (reservado) referido a afiliados, portafolios y transacciones de fondos de pensiones, información financiera de las administradoras u otra información que se encuentra directamente protegida por Ley deberán ser clasificadas como IBDE (ver sección 2).

Dentro de la información más comúnmente manipulada y requerida por el personal de la SP se encuentran las minutas internas, notas internas, información sobre entidades fiscalizadas, expedientes, oficios, estudios, bases de datos, información externa e informes de distinta naturaleza. Si bien dicha información puede no estar específicamente calificada por el

Comité de Planificación como IBDE, los funcionarios deberán ser cuidadosos en su tratamiento y manipulación debiendo observar como mínimo las disposiciones y recomendaciones establecidas en el Anexo 3 de este documento.

Cabe destacar que una parte importante de la información y bases de datos se encuentra bajo aplicaciones propias de la SP, preestablecidas y que permiten trabajar con acceso restringido. Sin embargo, existen una serie de aplicaciones particulares, elaboradas por las unidades usuarias y que manejan información confidencial (reservada) a través de planillas electrónicas de cálculo u otros programas de manejo de bases de datos. En estos últimos casos cobra especial relevancia el contenido de los siguientes acápites de esta sección.

3.3 Autorizaciones y Accesos a IBDE

Las autorizaciones para acceder a IBDE emanarán desde el Comité de Planificación y recaerán en las Divisiones correspondientes. Cada Jefe de División podrá autorizar a su personal a cargo, estando prohibido entregar autorización a personas que no pertenezcan formalmente a la institución. Las autorizaciones deben ser formales y comunicadas a la DAI por nota interna, especificando el motivo o justificación de la autorización, el nivel de acceso y/o las limitaciones cuando corresponda y el periodo por el cual se autoriza el acceso a la IBDE. El plazo de autorización no deberá exceder dos años y las personas autorizadas deberán firmar individualmente el compromiso de confidencialidad del Anexo 1, siendo responsabilidad de cada funcionario tramitar las renovaciones de los accesos a información. Una copia de este compromiso deberá quedar en poder del interesado y otra copia en la DAI.

La DAI creará y mantendrá actualizado un registro denominado "Registro de Accesos IBDE" en el cual se consignará la información clasificada como IBDE por el Comité de Planificación y las autorizaciones posteriores de acceso que se otorguen por parte del propio comité o por los jefes de división según corresponda. El Registro de Accesos IBDE será clasificado a su vez como IBDE, es decir, estará disponible para consulta a los funcionarios autorizados por el Comité de Planificación. No obstante, todo funcionario de la SP podrá consultar a través de su clave, el estado de sus accesos vigentes a IBDE.

En los casos en que ello sea posible, la DAI procurará la habilitación de sistemas automáticos de perfiles de "administrador" en los cuales se podrá otorgar los accesos a la IBDE jerárquicamente, es decir desde los jefes de división a los jefes de departamento y éstos a su vez al personal a su cargo, registrándose automáticamente los accesos y perfiles en el "Registro de Accesos IBDE".

En aquellos casos, en que técnicamente sea posible su implementación, se definirán niveles de acceso a la IBDE que deberán quedar consignados en el Registro de Accesos IBDE señalado en el 3.2 de esta sección. Los niveles de acceso podrán ser propuestos por los jefes de división o unidades usuarias de la información, especificando las restricciones /habilidades de los distintos niveles de acuerdo a las características propias de la IBDE que se trate. No obstante lo anterior, los niveles de acceso y las definiciones que se presentan a

continuación servirán de referencia para estructurar los niveles de acceso requeridos en cada situación y serán de uso obligatorio para otorgar los accesos en el caso de las bases de datos nominadas.

Nivel I (acceso total): Con este perfil de acceso se podrá consultar toda la información disponible sin restricciones y modificar la IBDE, cuando corresponda. La modificación o actualización de información corresponderá sólo en casos excepcionales y cuando la SP sea la generadora de la información (ejemplo; Calificaciones de la Matriz de Riesgos SBR). Cuando se permitan modificaciones a la IBDE, las aplicaciones deberán permitir el registro y la identificación de las modificaciones, indicando fecha, responsable y la modificación. Si estas modificaciones no se registraren automáticamente, la información deberá consignar en algún lugar identificado especialmente para estos fines y dentro de la misma IBDE dicha información (hoja especial con modificaciones, última actualización, etc.)

Las bases de datos que se estructuran a partir de información reportada por los organismos regulados, no deben ser modificadas directamente por personal de la SP (ejemplo: Base de Datos de Afiliados). Los sistemas deberán, cuando técnicamente sea posible, impedir la alteración de la información que fue reportada por un tercero. El mecanismo para actualizar o modificar información es la retransmisión o reenvío formal de la información a la SP por parte de los regulados o terceros informantes.

Nivel II (acceso restringido): El perfil de acceso Nivel II no permitirá bajo ninguna circunstancia modificar la información contenida en la IBDE, adicionalmente tendrá restricciones respecto a la información que la persona autorizada en este nivel puede acceder. El nivel de restricciones que presenta este acceso deberá quedar consignado en el Registro de Accesos IBDE que llevará la DAI y las aplicaciones informáticas que permitan operar con esta información deberán contener las restricciones coincidentes con las restricciones definidas para este nivel de acceso. En el caso de bases de datos nominadas, este perfil sólo permitirá acceder a información innominada. El proceso de innominación / nominación deberá ser efectuado por personas con acceso Nivel I y bajo un protocolo especial definido en conjunto por la DAI y la División de Estudios y publicado en la Intranet institucional.

Nivel III (acceso especial): Este perfil identificará tipos de acceso genéricamente distinto a los anteriores y se asignará a los usuarios que se les permita consultar información preestablecida o en la terminología de bases de datos de afiliados a "consultas semi-estructuradas". Así también, se deberá considerar este nivel de acceso para utilizar las aplicaciones que permiten búsqueda de personas (una a una por alguna variable predeterminadas, ej. RUT).

3.4 Clasificación y Rotulación de la Información

Independientemente de que la información haya sido calificada o no como IBDE, el personal responsable de la información de la SP deberá rotular la información sobre la cual tenga conocimiento que sea especialmente sensible ya sea desde un punto de vista legal o estratégico institucional. Para efectos de rotular la información y dar un tratamiento adecuado en cada caso, se deberá indicar claramente la naturaleza confidencial (reservada) de información o partes o campos que correspondan a información confidencial (reservada). No obstante, una base de datos o texto que contenga parcialmente información confidencial (reservada) deberá ser clasificada y rotulada en forma íntegra como "reservada". El criterio general para clasificar información debe procurar que el usuario siempre esté razonablemente enterado que está teniendo acceso a información confidencial (reservada). El Anexo 4 considera una "Guía para la Rotulación de la Información" y orienta sobre forma y avisos de confidencialidad.

Por motivos de seguridad no se puede asumir que aquella información que no está catalogada como "reservada" es pública, sólo aquella información rotulada explícitamente como "pública" tendrá esta naturaleza para efectos del manejo interno institucional/[6]. La información a la cual no se le haya asignado alguna de las clasificaciones anteriormente señaladas se asumirá como "reservada". La información reservada puede circular con esta denominación dentro de la SP con las restricciones de acceso que corresponda y para su conocimiento fuera de la institución requiere de autorización del Comité de Planificación o del Superintendente (ejemplo, minutas de temas en estudio, propuestas de normativa, etc).

Cuando un funcionario tenga dudas o discrepancias respecto a la clasificación de la información en las categorías mencionadas, deberá consultar a su superior y las consultas deberán ser canalizadas formalmente por los jefes de división o unidades al Comité de Planificación. El Comité de Planificación deberá responder formalmente a través de nota interna y si este comité lo considera pertinente, los alcances de la consulta podrán ser informados a más personas o a todo el personal de la institución.

/[6] Al respecto se debe tener en consideración la Ley de Transparencia, Ley N° 20.855.

4 Intercambio de Información con otras Instituciones

El intercambio de información con otras instituciones y/o personas cobra particular importancia dentro de este protocolo. Para facilitar el intercambio de información, a continuación se entregan algunos lineamientos básicos que se deberán respetar al momento de enviar o recepcionar una solicitud de información. La recomendaciones para un proceso de solicitud o flujo de información incluidas en el protocolo abarcan un "intercambio normal de información", entendiéndose que en determinadas circunstancias se enfrentan situaciones "extraordinarias o urgentes", las cuales deben ser resueltas a la brevedad pero que deberán necesariamente ser visadas directamente por el Superintendente o por quien designe para estos efectos.

4.1 Centralización de Solicitudes en la División de Estudios

La División de Estudios será la unidad encargada de canalizar todas las solicitudes de información desde y hacia la SP con personas naturales e instituciones no reguladas por la Superintendencia. En este rol, el Jefe de la División de Estudios deberá visar las solicitudes de información de esta naturaleza, generadas por las diferentes divisiones o unidades al interior de la SP, verificando su consistencia, no duplicidad con peticiones existentes de otras divisiones y los resguardos básicos contenidos en el presente protocolo. El oficio que contiene la solicitud de información será elaborado por la División solicitante, revisado por la Fiscalía y la División de Estudios (DE) y luego, la DE enviará el oficio a la firma del Superintendente.

En forma similar, las respuestas a solicitudes de información recibidas desde instituciones o personas externas a la SP deberán ser canalizadas a través de la División de Estudios, división que será responsable de coordinar con las instancias que corresponda, la evaluación de la solicitud considerando al menos los siguientes aspectos:

i) Factibilidad legal considerando las restricciones y facultades enunciadas en la Sección 2 de este documento (consulta a Fiscalía).

ii) Factibilidad técnica, referida fundamentalmente a la existencia de la información (periodos, variables y formatos solicitados), certeza o precisión de la información y capacidad de generación de la información, en el caso de que no se encuentre inmediatamente accesible. Dicha evaluación y potencial respuesta deberá ser aportada por la división que tiene acceso a la información o aquella que más cercanamente se encuentre relacionada al tema en consulta. Así también y dependiendo del tipo de solicitud, la factibilidad técnica deberá ser determinada o complementada con la evaluación de la DAI, así como también, la determinación de los medios seguros de transmisión.

La evaluación de las solicitudes deberá dimensionar el tiempo y los recursos potencialmente empleados en la elaboración de la información solicitada, con el fin de

facilitar las respuestas por parte de la SP. Se debe considerar que la generación de la información del tipo no habitual, con alta probabilidad, puede requerir la utilización de recursos extraordinarios para su elaboración, por lo que dichos recursos deben ser dimensionados, siendo este aspecto parte importante de la evaluación. Así también, la transmisión de dicha información o su transporte, puede involucrar requerimientos especiales de espacio o seguridad.

Se debe procurar responder en un plazo breve, teniendo en consideración la urgencia y pertinencia de la solicitud y eventualmente, los plazos preestablecidos reglamentariamente para responder (ej: Ley de Transparencia). Con todo, los plazos para responder, al menos en primera instancia, no deberán superar 30 días contados desde el plazo de recepción de la solicitud en la SP.

La respuesta enviada por la SP deberá indicar claramente, el carácter de público o reservada de la información enviada e indicar si corresponde, las restricciones que pudieran existir en el uso de dicha información. Asimismo, se deberá tener especial cuidado en la utilización de medios autorizados para el envío de información, procurando la utilización de los medios eficientes de mayor seguridad disponibles, en razón de las características de la información y el destinatario.

4.2 Medios Habilitados para el Intercambio de Información con Externos

Los medios que se enuncian a continuación son aquellos autorizados para el intercambio de información de acuerdo al presente protocolo. Los medios de transmisión están priorizados en razón de su seguridad o probabilidad de ser intervenidos por personas ajenas a aquellas que están autorizadas para intercambiar información. El uso específico de cada medio deberá ser evaluado caso a caso, dependiendo de si se trata de información periódica o puntual, de carácter reservado o público, de su clasificación como IBDE, de la urgencia del requerimiento, del costo del envío, etc. Para aquellos casos de mayor complejidad técnica, se deberá siempre solicitar la opinión de la DAI.

- Transmisión electrónica de datos: Cuando se trate de intercambios periódicos se deberá privilegiar la "transmisión de datos" a través de vías seguras. La situación más evidente en este sentido surge con las instituciones reguladas (IPS /AFPs /AFC). Para materializar dicha transmisión se deberá consultar la opinión técnica de la DAI, división que además coordinará los requerimientos para el proceso de transmisión. También se deberá privilegiar este mecanismo o similares técnicamente, cuando el intercambio de información se produzca con otros organismos estatales nacionales con los que exista intercambio regular de información/[7]. La información a intercambiar debe estar previamente definida y formalizada a través de una petición institucional.

/[7] Adicionalmente, en el caso de los organismos del Estado de Chile, la transmisión de datos debe apoyarse en las normas contenidas en el D.S. 81 del 2004 del Ministerio Secretaría General de la Presidencia. La transmisión puede realizarse a través de la Plataforma Integrada de Servicios Electrónicos del Estado (PISEE).

- Acceso sitio web: Cuando no se pueda establecer un proceso de transmisión segura de la información a través de una vía dedicada o exclusiva, se deberá optar por un acceso a través de clave a un sitio web definido para estos efectos. Por ejemplo, la SP podrá poner a disposición de la institución solicitante la información requerida en nuestro sitio web, con acceso a través de clave de usuario que deberá generar la DAI. Condiciones similares se deberán requerir en aquellos casos en que la institución solicitante sea la SP. La Superintendencia contará con una dirección URL en la que la institución informante podrá subir las bases de datos/[8]. La forma en que se accederá y habilitarán las claves de acceso deberán ser definidas por la DAI/[9].

- Medio portátil de almacenamiento con clave: Si no es posible o conveniente establecer una comunicación en los términos señalados anteriormente, se deberá enviar / recibir la información en un medio portátil de almacenamiento (ej, DVD, CD u otros), cuya información –de carácter reservada– sólo pueda ser accesible con la utilización de una clave. El dispositivo deberá ser enviado al jefe del servicio o directivo superior de la Institución (directamente al Superintendente cuando se trate de recepción de información), en un sobre sellado, identificando además la división y el destinatario de la información. Los medios de transporte válidos de entrega serán: entrega personal (acreditando recepción), correo certificado y correo personalizados tipo *express*.

- Información en papel: Si no hay alternativa o se ha determinado que la información estará impresa en papel, los medios de transporte válidos para enviar / recibir la información serán los mismos señalados en el párrafo anterior, tomando aquellos resguardos razonables para el transporte de la información (indicando que se trata de información reservada, utilizando un sellado apropiado, evitando que se trasluzca, etc.).

- Correo electrónico: El correo electrónico nunca deberá ser utilizado para el envío de información periódica. Sólo se podrá enviar información por correo electrónico cuando lo autorice el Superintendente en razón de la urgencia y/o imposibilidad de actuar distinto. En el caso de información de carácter reservada, se deberá enviar la información en forma cifrada, en tanto que para la información recibida por este medio, se deberá solicitar al destinatario (de ser factible para él) su envío en forma cifrada, En el caso que esté disponible, se deberá usar la firma electrónica con certificado digital.

/[8] La DAI definirá un tamaño máximo de bases de datos a subir a través de la dirección URL.

/[9] Notar que la base de datos será subida a la dirección URL utilizando una transmisión encriptada hasta que llegue al servidor de la Superintendencia de Pensiones.

5 Acceso de Externos a Información SP

Existen situaciones especiales en que personas externas a la SP tendrán acceso autorizado a la IBDE u otra información que se maneja en la institución. En esta situación se encuentran las personas contratadas a honorarios, alumnos en práctica, profesionales en pasantías o delegaciones extranjeras, académicos realizando investigación conjunta con la SP u otros profesionales contratados por la SP. En todos estos casos, la DAI debe encargarse que las personas firmen una declaración de responsabilidad y de confidencialidad de la información a la cual tengan acceso en razón de las actividades que estén desempeñando en la SP, la cual incorpora el compromiso de respetar el presente Protocolo de Manejo Responsable de Información (Anexo 2: Acuerdo de Confidencialidad Persona Externa a la SP).

Independiente de la firma del acuerdo de confidencialidad, las personas anteriormente señaladas deberán contar con una autorización expresa para acceder a información reservada extendida por el Comité de Planificación o por quien designe. En dicha autorización deberá quedar establecido el acceso a IBDE, el nivel de acceso y la firma de la persona que autoriza. Asimismo, la autorización deberá quedar consignada en el Registro de Accesos IBDE de la SP.

En términos generales las personas externas a la SP deberán cumplir con estrictas medidas de seguridad en el manejo de información. En el caso que la Superintendencia subcontrate o externalice estudios técnicos o actuariales en los que sea necesario utilizar el universo completo de alguna de las bases de datos, los investigadores externos deberán trabajar en las dependencias de la Superintendencia en *computadores restringidos,* especialmente adaptados para resguardar razonablemente la seguridad de los datos a los cuales se tiene acceso (sin acceso a internet ni a e-mail, sin puerto USB, ni tener la posibilidad de copiar la información). Los investigadores o personas externas a la SP nunca podrán acceder a las bases de datos nominadas, ya sea el universo total o una muestra, como resultado de los procesos que se desarrollen en las dependencias de la Superintendencia. Sólo podrán disponer de resultados agregados tales como cuadros estadísticos, resultados econométricos o datos innominados.

Al término de las labores desempeñadas en la SP, las personas deberán devolver al Jefe de la División encargada, todo el material al que han tenido acceso en la SP y/o eliminar las copias con información total o parcial que pudieran tener en su poder. El uso de información, como asimismo de las conclusiones o resultados obtenidos en razón del trabajo en la SP o en colaboración con la SP debe ser autorizado expresamente por el Superintendente.

Anexo 1: Acuerdo de Confidencialidad Personal SP

Acuerdo de Confidencialidad

Santiago, XX de XXX de 20XX

Yo, **<nombre completo>,** RUN <run> o N° Pasaporte < número>, funcionario en calidad de <contrata/planta> de la Superintendencia de Pensiones de Chile, en adelante SP, en mi desempeño del cargo de <cargo/unidad/dpto./división>, suscribo el presente Compromiso de Confidencialidad.

En el ejercicio de mis tareas funcionarias puedo tener acceso a múltiples tipos y formas de información relacionadas con la SP y otras entidades que forman parte del Estado de Chile, como también de entidades privadas, sus accionistas, directores, proveedores, empleados y clientes, que sean o no objeto de fiscalización por parte de la SP.

En particular tendré acceso a la información confidencial o reservada que se identifica a continuación:

a) XXXXX
b) XXXXXXXX
c) XXXXXXX

Entiendo que toda la información no pública relacionada con las personas y entidades mencionadas tiene el carácter de confidencial o reservada, está sujeta a reserva de mi parte y sólo puedo utilizar la información para los fines que mis responsabilidades como funcionario de la SP requiera.

Entiendo que en algunos casos, la publicación, traspaso no autorizado o mal uso de información confidencial o reservada puede ser un crimen penado por Ley. Entre las normas más relevantes al respecto se encuentran las Leyes Nro. 19.628, 19.728 y 20.255 y el DL 3.500 y otras disposiciones mencionadas en la Sección 2 del Protocolo de Manejo Responsable de Información de la SP.

Además, declaro conocer y me comprometo a respetar las disposiciones del Código de Ética de la SP, comunicado a través de la Resolución Exenta N° 1440 de fecha 20 de agosto 2010 y el Protocolo de Manejo Responsable de Información de la SP.

Me comprometo a:

- No divulgar información confidencial o reservada, por ningún medio, sin un permiso escrito de la SP.
- Entregar mi mayor esfuerzo para proteger la información confidencial o reservada de ser divulgada o mal utilizada.
- Usar sólo la información confidencial o reservada para el propósito de mi trabajo en la SP; y Devolver a la SP cualquier información confidencial que pueda tener en mi poder cuando termine mi trabajo en la SP, o antes si la SP así me lo solicita.
- Poner en conocimiento a la jefatura directa de cualquier situación o incidente que se divulgue o comprometa la confidencialidad de la información.

Firma del testigo de la SP
Nombre:

.....

Firma del Funcionario de la SP que suscribe compromiso

Nombre:

.....

Anexo 2: Acuerdo de Confidencialidad Persona Externa a la SP

Acuerdo de Confidencialidad

Santiago, XX de XXX de 20XX

Yo, YYYY YYYYY YYYYY, nacionalidad (XXXX), Rut: XXXXXXX –X / N° pasaporte XXXXXX, desarrollaré labores en la Superintendencia de Pensiones, en calidad de alumno en práctica /investigador tiempo parcial a partir del X de XXXX de 201X y hasta el XX de XXXX de 201X (o meses). El principal objetivo de esta contratación / pasantía será .....

Declaro estar en pleno conocimiento que la información a la cual tendré acceso o podría tener acceso en la Superintendencia de Pensiones es de carácter confidencial o reservada y su uso o divulgación está sujeta a sanciones establecidas por Ley. Asimismo, declaro conocer las condiciones de acceso y uso de información, contenidas en el documento "Protocolo para el Manejo Responsable de Información" de la Superintendencia de Pensiones, así como también, conocer las disposiciones del "Código de Ética" de la institución, las cuales me comprometo a respetar a cabalidad.

Por último, declaro estar en conocimiento que el material elaborado a partir del trabajo desempeñado en la Superintendencia y los potenciales resultados o conclusiones que pueda obtener son de propiedad de la Superintendencia de Pensiones y su uso bajo cualquier circunstancia requiere expresa autorización de dicha institución.

YYYY YYYYY

Anexo 3: Recomendaciones para la Manipulación y Almacenamiento de Información

Las recomendaciones que se establecen en este anexo no agotan los potenciales resguardos que se puedan adoptar en función de proteger la información que manejan los profesionales en la SP. Por ello, las personas deben proceder con un criterio de prudencia que en muchos casos y dependiendo de las circunstancias, implica adoptar resguardos superiores a aquellos aquí consignados. Las siguientes recomendaciones constituyen un mínimo a aplicar y deben ser complementadas con las recomendaciones o procedimientos especiales señalados en los manuales de procedimientos elaborados por las unidades especializadas respectos de determinadas actividades y/o procesos.

- Nunca compartir claves, especialmente si ellas permiten tener acceso a información confidencial (IBDE).
- Cambiar las claves a lo menos cada seis meses procurando que ellas cumplan estándares de seguridad para gestión de claves (alfanuméricas, de largo predeterminado, sin información personal, entre otras).
- No usar programas ni aplicaciones no autorizadas por la institución.
- No acceder a copias de información o bases de datos confidenciales o reservadas a los cuales no se tiene acceso autorizado.
- No generar copias totales o parciales de información catalogada como IBDE que puedan circular o manipularse sin el nivel requerido de resguardo o facilitar su uso por personas no autorizadas.
- No dejar documentos impresos abandonados en las impresoras, fotocopiadoras o en lugares sin acceso restringido (salas de reuniones / otras oficinas).
- Dar aviso y/o entregar a las secretarias de división, información que pueda ser encontrada en lugares de acceso general.
- Eliminar información grabada en notebooks de sala de reuniones u otras dependencias, asegurando también su eliminación de la papelera.
- Trasladar información confidencial/ reservada, incluso dentro de las dependencias de la SP, con medidas de resguardo, tales como sobre sellados, carpetas cerradas e indicando visiblemente el carácter de reservada de la información.
- Destinar algún mueble o lugar para almacenar información que pueda ser catalogada como IBDE. Este lugar puede ser individual o determinado por la División o / Unidad correspondiente para estos efectos.
- No usar e-mail para el envío de información confidencial/reservada fuera de la SP. Solo utilizar el e-mail si es estrictamente necesario y si se cumplen las condiciones señaladas en la Sección 4.2 de este documento. Considerar el uso de firma electrónica existente en la SP.
- No utilizar el disco duro del computador personal para grabar la información institucional y utilizar exclusivamente como dispositivo de almacenamiento los discos o unidades de red que la DAI determine para estos efectos (ejemplo: disco F), los cuales corresponden a servidores protegidos y respaldados.
- Mantener el escritorio libre de documentación confidencial/reservada o IBDE, la cual preferentemente deberá guardarse en muebles con llave.

- No transportar información confidencial/reservada fuera de la oficina.

  No usar dispositivos de almacenamiento portátiles (e.g., pendrive / CD / DVD / discos externos USB / notebook, etc.) para transportar información confidencial o reservada fuera de la oficina. Evitar trasladar información confidencial/reservada fuera de la oficina y por motivos distintos a realizar labores de trabajo (reuniones o trabajo extraordinario y justificado).
- Enviar información reservada en sobres debidamente sellados utilizando los medios de transporte y protocolos autorizados.
- Se podrán utilizar accesos remotos a información de la SP, estando debidamente autorizado por el CP.
- Utilizar bloqueadores de pantalla en los puestos de trabajo que permitan bloquear el acceso, si no hay actividad, en un plazo reducido (recomendado 15 minutos). Apagar los computadores al finalizar la jornada laboral.
- Dar la categoría de información reservada a la IBDE que circule por el Sistema de Gestión Documental (SGD).

Anexo 4: Guía para la Rotulación de la Información Confidencial/Reservada (Templates)

El objetivo de este Anexo es entregar una guía para rotular adecuada y visiblemente la información confidencial/reservada o IBDE con el objetivo de que cualquier persona se entere razonablemente que está accediendo a información confidencial/reservada. La recomendación es siempre disponer de medidas de seguridad en el acceso a esta información, tales como utilización de claves, sistemas especiales, lugares físicos resguardados, etc. No obstante, al acceder a esta información, los usuarios deben informarse adecuadamente del carácter de confidencial/reservada de la información.

Una guía actualizada para Rotular Información IBDE estará disponible en Intranet, donde se podrán obtener *templates* institucionales para presentaciones, minutas, subject de e-mail, oficios reservados, sobres y carpetas con información confidencial/reservada, rotulación para planillas electrónicas y advertencias tipo para aplicaciones desarrolladas en nuestra institución.

a) Minutas Internas

En cada página como encabezado: Reservada

MINUTA DIVISIÓN XXXXX **ROTULACIÓN DE INFORMACIÓN RESERVADA** (Folio o Numeración Interna a la División)

Depto. de XXXXXX
Juan XXXX/ Rodrigo XXXX
XX de octubre de 201X

RESERVADA

Materia: XXXXXX XXXXXXXX .

Texto de la Minuta…..

Página numerada

b) Documentos (Tapa)

En cada página como encabezado: Reservada

ROTULACIÓN DE INFORMACIÓN

Superintendencia de Pensiones

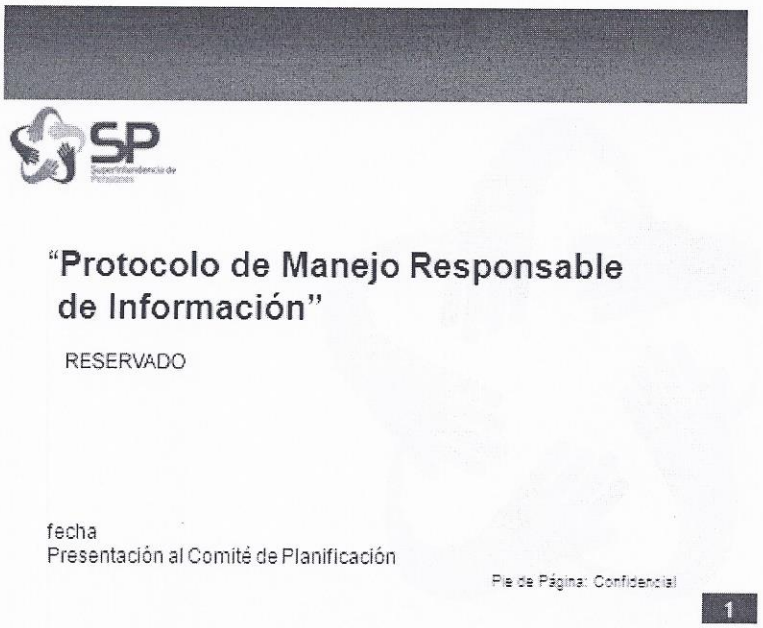
Fecha

RESERVADA

Sólo para comentarios SP

Versión 2.0

c) Presentaciones



d) E- mail

Respecto de los e-mails con información confidencial/reservada enviados dentro de la institución estos deberán cumplir con la condición de iniciar el asunto o subject con la palabra IBDE o reservada.

Asunto: Confidencial datos XXXXXXX o Asunto: IBDE datos XXXXXXX

Se debe tener en consideración para no rotular todo como reservado que la rotulación indicada del asunto del e-mail se utilizará sólo en el caso en que los adjuntos contengan información confidencial/reservada. En el caso que no exista adjunto y la información del texto o cuerpo del e-mail tenga el carácter de confidencial/reservada, en alguna parte del texto se debe señalar este hecho con la palabra "Confidencial". Cuando sea posible, indicar en el texto principal de e-mail, el nombre del destinatario para facilitar la identificación de aquellos correos recibidos por error en la dirección.

En aquellos casos en que se reenvíe información externa o un e-mail recibido desde personas o instituciones ajenas a la SP con carácter de confidencial/reservada se deberá indicar la palabra "confidencial".

Si algún funcionario recibiere por error un correo electrónico de otro funcionario con información confidencial/reservada deberá notificar este hecho por la misma vía al emisor del correo y luego eliminar el mensaje de la bandeja de entrada y posteriormente de la carpeta que contiene los correos eliminados.

En los correos electrónicos enviados a personas externas a la SP, se deberá tener especial consideración de las instrucciones de la sección 2.4 del presente documento. Sin perjuicio de lo anterior, se deberá enviar los correos utilizando un asunto que **no** entregue indicación del carácter de confidencial/reservada de la información y, por lo tanto, no se deberá utilizar la palabra confidencial, IBDE o reservado.

Adicionalmente se deberán respetar las siguientes indicaciones:

- En el texto del correo se deberá identificar al destinatario con su nombre
- Se deberá agregar una nota al final del correo que indique:
  Nota: Información confidencial/reservada de la SP para uso exclusivo de << nombre de la institución receptora>>.
- Se debe incluir una leyenda que advierta al receptor por error de esta información su responsabilidad legal de acceder a esta información, su obligación de notificación al emisor y de su eliminación.
- Adjuntar archivos cuidando que su rotulación cumpla con las indicaciones de este anexo dependiendo del tipo de archivo que se trate.

e) CD o DVD

Los discos utilizados con IBDE deberán utilizar etiquetas especiales tanto en el propio disco como en su caja de almacenamiento. Se debe recordar que estos medios con información IBDE deberán estar siempre con clave para el acceso a su información. Las etiquetas deberán estar disponibles para su impresión en las secretarías de las divisiones en conformidad con el siguiente formato.

f) Información en papel

Dada la diversidad de situaciones o formas en las que se puede presentar la información impresa resulta imposible abarcar todos los casos, por lo que se deberá siempre utilizar una asimilación razonable a los casos aquí presentados.

- Considerar la utilización de los formatos señalados en las letras a) y b) del presente anexo. Privilegiar el uso de primeras páginas /tapas que no revelen contenido específico confidencial/reservada (sólo indiquen que contiene información confidencial/reservada).

- Cuando se trate de oficios reservados elaborados por la SP se deberá indicar esta calidad en la parte superior derecha del oficio usando el formato habitual de la SP del cual disponen las secretarias en la institución.

- El ingreso de oficios reservados al Sistema de Gestión Documental (SGD) de la SP debe ser registrado en calidad de reservado con la aplicación existente en el SGD para estos efectos.

- Si se trata de información ya impresa o histórica que no consigne la calidad de confidencial/reservada, cuando ello corresponda y no constituya una alteración al valor legal o documental histórico de dicha información, agregar visiblemente un timbre con la leyenda "Reservada".

- Si no es posible agregar una marca de timbre en los términos señalados en el punto anterior o no resulta eficiente hacerlo, se debe utilizar una carpeta, sobre o dispositivo contenedor de esta información, rotulado con una etiqueta visible que indique su carácter de "Reservada".

g) Mensajes de Advertencia en Software y Archivos Electrónicos

En las aplicaciones informáticas desarrolladas internamente en la SP se deberá habilitar un mensaje de advertencia respecto del acceso a la información confidencial/reservada, sin perjuicio de las medidas de seguridad que pudieran tener implementadas dichas aplicaciones en conformidad con este Protocolo de Uso Responsable de Información.

En este sentido, cuando técnicamente sea factible de implementar, se debe incorporar un mensaje visible que se despliegue, una vez superado el proceso de introducción de nombre de acceso y claves que permiten el ingreso a las aplicaciones. El mensaje debe incorporar opciones de aceptar el ingreso o salir de la aplicación.

El mensaje de advertencia deberá tener el siguiente formato:

Advertencia

Acceso a Información Reservada

- Estoy debidamente autorizado por la Superintendencia de Pensiones para utilizar esta aplicación informática y acceder a la información confidencial/reservada con la cual trabaja este programa.
- Acepto las condiciones y consecuencias de las regulaciones que rigen el acceso a la información confidencial/reservada a la cual estoy accediendo a través de esta aplicación.

ACEPTAR CANCELAR

En el caso de archivos de paquetes estadísticos y/o aplicaciones tradicionales con licencia comercial se deberá indicar en la primera hoja o línea la frase: "Información Reservada". A modo de ejemplo, en una planilla electrónica de cálculo se deberá indicar la frase referida, visiblemente en la primera fila de cada hoja. Las pantallas de salida o "output" a imprimir también deberán incluir la rotulación "Información Reservada".