APRUEBA LA "POLÍTICA DE CONTROL DE ACCESO A LA INFORMACIÓN FÍSICA Y DIGITAL", INSERTA EN EL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO DE PREVISIÓN SOCIAL, APROBADA POR RESOLUCIÓN EXENTA N° 657, DE 2015.

RESOLUCIÓN EXENTA Nº 345

SANTIAGO, 18 JUL 2016

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.- 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.

CONSIDERANDO: 345

1.- Que, por Resolución Exenta Nº 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 en forma permanente por los funcionarios que desempeñan los cargos de Subdirectores, Jefes de las Divisiones Jurídica, Informática, Planificación y Desarrollo, Beneficios y por el Encargado de Seguridad de la Información, dejando establecido la participación como invitado del Director Nacional, Jefe División Contraloría Interna, Jefe del Departamento de Personas y el Jefe del Departamento Compromisos Institucionales.

3.- Que, mediante Resolución Exenta N°170, de 10 de abril de 2015, se 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, correspondiéndole actuar como asesora de esta Dirección Nacional para velar por preservar la confidencialidad, integridad y disponibilidad de la información, de conformidad con las normas legales y reglamentarias sobre la materia.

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 propuesto el texto denominado "Política de Control de Acceso a la Información Física y Digital", con la finalidad de proporcionar seguridad respecto a la integridad y seguridad de los sistemas y recursos de información física y digital del Instituto de Previsión Social, que incluye los textos complementarios: "Política Pantallas y Escritorios Limpios" y "Política de Claves de Acceso de los Sistemas Informáticos".

6.- Que, asimismo por Oficio Ordinario N°45128/2301-2016, de 13 de junio de 2016, la División Jurídica de este Instituto, aprueba y visa en cada una de sus páginas el proyecto denominado **"Política de Control de Acceso a la Información Física y Digital"**, aprobado por el Comité de Seguridad de la Información, en sesión de fecha 04 de mayo de 2016, según consta en Acta de Reunión enviada por la Encargada de Seguridad de la Información, a través documento electrónico de 22 de junio de 2016, estableciendo la procedencia de emitir la Resolución aprobatoria de rigor, la que de conformidad a la Resolución N°1.600, de 2008, de la Contraloría General de la República, que fijó normas sobre exención del trámite de Toma de Razón, se encuentra exenta del mencionado trámite.

R E S U E L V O:

1.- Apruébase, para el Instituto de Previsión Social la **"Política de Control de Acceso a la Información Física y Digital"**, que incluye los textos complementarios: "Política Pantallas y Escritorios Limpios" y "Política de Claves de Acceso de los Sistemas Informáticos", que consta de quince (15) páginas, que se adjunta como parte integrante de la presente Resolución Exenta, con aprobación legal de fecha 13 de junio de 2016, cuyo objetivo es proporcionar seguridad respecto a la integridad y seguridad de los sistemas y recursos de información, a través de un adecuado manejo y mantenimiento de las cuentas del usuario, los derechos y privilegios asociados a ellas, las cuales permiten acceder a los servidores, aplicaciones y bases de datos, restringiendo el acceso a la información y a las instalaciones de procesamiento de la información.

2.- Déjese sin efecto, el Resuelvo N°2, Punto N°7, "Política de Control de Accesos a la Información", de la Resolución Exenta N°591, de 28 de diciembre de 2009, instrumento que permanece vigente, en todo lo no modificado por el presente acto administrativo.

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".

4.- 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 PREVISION SOCIAL
DIRECTOR NACIONAL

PATRICIA 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

MEES/AVA/YGE/MRH/YGC/[illegible]/WNCR/ MAGA/RES/MRC/mrc
Aprueba "Política de Control de Acceso a la Información Física y Digital
VI- (Folio DTD-3575-104)

POLÍTICA DE CONTROL DE ACCESO A LA INFORMACIÓN FÍSICA Y DIGITAL

CODIGO: POL-08

INCLUYE
POLÍTICA PANTALLAS Y ESCRITORIOS LIMPIOS
POLÍTICA DE CLAVES DE ACCESO DE LOS SISTEMAS INFORMÁTICOS

CONTROL DE CAMBIOS

Fecha	Versión	Página	Numeración del contenido	Cambio Efectuado/Nombre del responsable
03/09/2015	02	Todas	Todo	Modificación de nombre de política y ajuste debido a versión de la norma ISO Nch27001:2013
28/12/2009	01			Versión original Resolución Exenta N°591 del 28-12-2009

(*) 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.

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.

ÍNDICE

1. OBJETIVO

Proporcionar seguridad respecto a la integridad y seguridad de los sistemas y recursos de información, a través de un adecuado manejo y mantenimiento de las cuentas del usuario, los derechos y privilegios asociados a ellas, las cuales permiten acceder a los servidores, aplicaciones, bases de datos, restringiendo el acceso a la información y a las instalaciones de procesamiento de la información.

2. ALCANCE

Se aplica a todos los sistemas de información del Instituto de Previsión Social IPS, bases de datos, software, equipos, instalaciones, sistemas, y redes que la organización posee, de manera que la no inclusión explicita en el presente documento, no constituye argumento para no proteger los activos de información que se encuentren en otras formas.

Se aplica a quienes trabajen en el IPS, independiente de su modalidad de contratación, funcionarios de planta, contrata, honorarios, asesores, consultores, alumnos en práctica, incluyendo a personal de empresas externas.

Incluye toda la información impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o usando medios electrónicos, mostrada en películas o hablada en una conversación.

3. DOCUMENTOS DE REFERENCIA

CONTROL LEGAL Y NORMATIVO

República de Chile

- Código Penal de la República de Chile.
- Circular N° 3, enero de 2007, de los Ministerios del Interior y de 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.
- 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.

República de Chile

- Decreto 779, noviembre 2000, reglamento del registro de bancos de datos personales a cargo de organismos públicos.
- Decreto 277. Reglamento de Propiedad Intelectual.
- 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.
- 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.
- La Constitución Política de la República de Chile.
- Instructivo Presidencial N°4, junio de 2003: Imparte instrucciones sobre aplicación de la Ley de Bases de Procedimientos Administrativos.
- 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, cuyo texto refundido fue fijado por el D.F.L N° 29, de 2004, del Ministerio de Hacienda.

	POLÍTICA DE CONTROL DE ACCESO A LA INFORMACIÓN FÍSICA Y DIGITAL		SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
	Nivel de Confidencialidad	**Interno**	Versión: 2 Fecha de Aprobación Legal: 13 JUN 2016 Página: **6 de 15**

República de Chile

- 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, agosto de 1999, sobre "Protección de la Vida Privada y Datos Personales", Ministerio Secretaria General de la Presidencia.
- Ley Nº 17.336, octubre de 1970, sobre "Propiedad Intelectual", Ministerio de Educación.
- Ley Nº 19.223, junio de 1993, sobre "Delitos informáticos" del Ministerio de Justicia.
- Ley N°19.799, abril de 2002. 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.
- 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.

NCh-ISO 27001:2013

A.9.1.1 Política de control de acceso.

A.9.1.2 Accesos a las redes y a los servicios de la red.

A.9.2.1 Registro y cancelación de registro de usuario.

República de Chile
A.9.2.2 Asignación de acceso de usuario.
A.9.2.3 Gestión de derechos de acceso privilegiados.
A.9.2.4 Gestión de información secreta de autentificación de usuarios
A.9.2.5 Revisión de los derechos de acceso de usuarios
A.9.2.6 Eliminación o ajuste de los derechos de acceso
A.9.3.1 Uso de información de autenticación secreta
A.9.4.1 Restricción de acceso a la información
A.9.4.2 Procedimiento de inicio de sesión seguro
A.9.4.3 Sistema de gestión de contraseñas
A.9.4.4 Uso de programas utilitarios privilegiados
A.9.4.5 Control de acceso al código fuente de los programas

REFERENCIAS

Documentos Internos	
Título	**Nombre del archivo**
Política General de Seguridad de la Información	Política General de Seguridad de la Información.pdf

4. DEFINICIONES

Activo de información: Los activos de información son todos los elementos 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, infraestructura y datos.

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 la normativa vigente.

Correo Electrónico: es un servicio de red que permite a los usuarios enviar y recibir mensajes mediante sistemas de comunicación electrónica. Principalmente se usa este nombre para denominar al sistema que provee este servicio en Internet, mediante el protocolo SMTP. Por medio de mensajes de correo electrónico se puede enviar, no solamente texto, sino todo tipo de documentos digitales dependiendo del sistema que se use. Su eficiencia, conveniencia y bajo costo están logrando que el correo electrónico desplace al correo ordinario para muchos usos habituales.

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. Responsable de velar por el cumplimiento de las políticas de seguridad de la información, sus normas y procedimientos. Asesora al Director Nacional en materia de Seguridad de la Información, y dirige el Comité de Seguridad de la Información.

Incidente de seguridad: Situación adversa que pone en riesgo un proceso.

Información: es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Medios: es el instrumento o forma de contenido por el cual se lleva a cabo el proceso de la comunicación.

Mantenimiento: todas las acciones que tienen como objetivo mantener un articulo o restaurarlo a un estado en el cual pueda llevar a cabo alguna función requerida. Estas acciones incluyen la combinación de las acciones técnicas y administrativas correspondientes.

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.

Red: una red de computadoras, de comunicaciones, de datos o red informática, es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos

eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Transferencia de Información: método generado con la intensión de agilizar y automatizar la entrega e intercambio de información de forma segura, la cual permite el envío de cantidades masivas de información.

5. RESPONSABILIDADES

- **Comité de Seguridad de la Información CSI:** Responsable de la revisión de esta política cada 3 años o cuando la situación lo amerite. Además debe implementar los medios y canales necesarios para que la Encargada de Seguridad pueda difundir esta política.
- **Departamento de Administración e Inmobiliaria:** Debe crear y supervisar los procedimientos necesarios para asegurar el ingreso y el acceso a las dependencias en los que se encuentren los activos de información (bodegas, oficinas y otros)
- **Departamento de Seguridad de Información:** debe elaborar los procedimientos que garanticen un correcto acceso a la información de IPS, además debe resguardar el control del mencionado acceso.
- **División de Informática:** Debe velar por el cumplimiento de esta política, y de los procedimientos que se relacionan con ella, en el control de accesos a la información.
- **División de Beneficios y responsables del proceso**: deben proteger y respetar los procedimientos para el control de accesos a los activos de información.
- **División Jurídica**: Debe aplicar el proceso disciplinario formal, y sabido por los funcionarios para tomar acciones en contra de los que hayan cometido una infracción a la seguridad de la información.

POLÍTICA

5.1 Se debe restringir a funcionarios no autorizados el acceso a determinados sectores, oficinas, áreas de trabajo que contienen información sensible. En los casos de sala de servidores y "data center", estos tendrán procedimientos específicos de acceso, y una nómina de funcionarios autorizados. De igual manera, las salas que contengan equipos de comunicaciones, switch, PBX, routers, consolas de administración serán controladas en sus accesos y revisados según procedimientos definidos.

5.2 Todo funcionario del IPS debe utilizar su credencial de identificación en horas de trabajo. Esto permite su identificación en las distintas dependencias, en los casos que se requiera, se utilizará control biométrico.

5.3 Los accesos físicos a la División Informática deben estar controlados y supervisados por un guardia y/o control biométrico.

5.4. Los funcionarios que cuentan con el acceso a información estipulada como clasificada, tienen prohibida su difusión, sea ésta a través de su venta, traslado, etc. El funcionario que transgreda esta política, se sancionará con lo establecido en el Estatuto Administrativo y la política de Seguridad de Recursos Humanos.

5.5 Todo requerimiento de información de la organización como comunicados públicos, declaraciones, cuestionarios, encuestas o entrevistas periodísticas, deben ser referidos al Departamento de Comunicaciones de IPS.

5.6 Debe existir un procedimiento para el registro y eliminación de usuarios, para garantizar que se otorguen y quiten accesos a los sistemas de información. Este procedimiento debe revisar los derechos de ingreso a la red, correo y sistemas, con su respectivo registro de usuarios, identificando otorgamientos y bajas. Los accesos a sistemas deben tener procedimientos de autenticación seguros, y revisión de estos permisos, de modo de minimizar la oportunidad de accesos no autorizados.

5.7 Cuando un funcionario deja su puesto en la institución, los archivos residentes en los computadores y los archivos impresos, deben ser revisados por algún funcionario con las facultades para realizar dicha acción, para una reasignación formal de las tareas pendientes. En los casos de cese de funciones o cambio ellas, o modificación de contrato, se debe retirar o modificar sus derechos de acceso a los sistemas de información de forma inmediata, para que no exista posibilidad de robo o fuga de información.

5.8 Los funcionarios no deben utilizar herramientas para obtener información de la red, como detección de puertos, servicios y archivos en general en los sistemas de información de IPS.

5.9. Se debe solicitar a los usuarios firmar una declaración en que mantengan la información de autenticación secreta de manera personal y que mantengan la información de autenticación secreta grupal, dentro de los miembros del grupo.

5.10 El acceso lógico a la configuración de puertos de manera remota debe ser controlado. Se deben establecer procedimientos de autenticación para los usuarios que utilicen accesos remotos. Por ejemplo: Utilización de protocolos de autenticación y autorización como Radius, esquemas de autentificación como PAP, CHAP o EAP, integración con repositorios de usuarios del IPS (por ejemplo: LDAP o bases de datos de usuarios) y accesos seguros a través de VPN IPSEC o SSL (se sugiere VPN para accesos fuera del perímetro del IPS).

5.11 No se debe utilizar cuentas genéricas para acceder a los sistemas de IPS, como tampoco utilizar ninguna estructura de contraseña que resulte predecible o fácil de adivinar, esto incluye contraseñas en blanco y secuencias comunes de caracteres con excepción de los Sistemas Reforma, Core Agil y Legados.

5.12 Todos los usuarios deben autenticarse con Usuario y Contraseña válidos antes de usar sistemas de información de IPS. Todo funcionario debe cambiar cada 3 meses su contraseña, lo cual será recordado a nivel de software. Los intentos fallidos de conexión serán registrados. No se mostrará la contraseña ingresada.

5.13 Las contraseñas fijas no deben ser almacenadas en archivos de ejecución por lotes, scripts automáticos, macros de software, computadoras de control de acceso o en otros medios donde personas no autorizadas pueden conocerlas. Tampoco deben ser escritas o almacenadas en lugares visibles o cerca de los sistemas a los cuales permiten el acceso. Debe existir un procedimiento de administración de contraseñas.

5.14 Todo funcionario debe dejar su equipo bloqueado en caso de no estar en su lugar de trabajo, cerrada su sesión de correo, y cerradas las sesiones de sistemas de IPS.

5.15 Ningún usuario final debe tener privilegios de usuario administrador, o permisos para acceder al código fuente de los programas, salvo funcionarios que realizan funciones que lo requieran.

5.16 Todo equipo de trabajo debe ser apagado una vez que el funcionario termine su jornada de trabajo. Los notebooks, tablets y celulares asignados, según su modalidad de trabajo y formulario de entrega, deben guardarse en lugares seguros.

5.17 Todo equipo de trabajo de IPS debe estar configurado con protector de pantalla con contraseña.

5.18 Si un funcionario tiene que dejar su computador personal encendido y conectado a la red fuera de horario de oficina, este equipo debe contar con sistema de seguridad aprobado e informado a

la unidad correspondiente en la DTI. Asimismo, las sesiones que se encuentren inactivas serán desconectadas después de un periodo definido de inactividad.

5.19 Las actividades que afectan información sensible, de sistemas en producción, deben ser reconstruibles a partir de registros de transacciones. Para ello cada responsable de proceso debe velar porque existan procedimientos de respaldo de información, los cuales deben estar identificados en un registro de la División de Informática.

5.20 Las herramientas de monitoreo de actividades computacionales se usarán sin una notificación previa a los usuarios involucrados. Se incluyen las investigaciones de actividades criminales.

5.21 Los mensajes enviados por el sistema electrónico de correo de IPS, sólo pueden ser leidos bajo los requerimientos establecidos en la normativa legal, en caso de persecución criminal o administrativa.

5.22 Antes de otorgar permisos de trabajo remoto a funcionarios de IPS, se debe firmar un acuerdo de confidencialidad que proteja la información sensible de la institución, y cumplir con el procedimiento establecido para ello. El acceso a información confidencial, puede ser otorgado de manera individual o grupos de usuarios.

5.23 Debe existir un procedimiento que regule el manejo y mantenimiento de certificados digitales, incentivando su uso.

5.24 El Comité de Seguridad de la Información debe promover con capacitaciones a los usuarios, las buenas prácticas en la red y sus equipos.

5.25 La DTI debe publicar en los accesos de sus instalaciones y en la Intranet, los instructivos relativos a uso de redes y servicios de red.

POLÍTICAS COMPLEMENTARIAS

6. POLÍTICA PANTALLAS Y ESCRITORIOS LIMPIOS

6.1 Los escritorios deben permanecer limpios de documentos en papel y dispositivos de almacenamiento removibles como CD, DVD, cintas, pendrive, etc.

6.2 Todos los computadores personales y notebooks deben protegerse con protectores de pantalla con contraseña, configurando la activación automática de este bloqueo en menos de 10 minutos, o bien

desconectándose del computador (presionando control-alt-delete en los computadores con las versiones de Windows correspondientes) cuando el computador quede desatendido por un tiempo.

6.3 Los documentos en papel y medios informáticos deben ser almacenados bajo llave en gabinetes y/u otros tipo de mobiliario seguro, cuando no están siendo utilizados, especialmente fuera del horario de trabajo.

6.4 Se recomienda que la información reservada del Instituto se guarde bajo llave (preferentemente en caja fuerte) cuando no está en uso, especialmente cuando no hay funcionarios en la oficina.

6.5 Los reportes o impresiones que tengan información de uso interno o reservado deben ser destruidos antes de tirarlos en depósitos de basuras.

6.6 Se recomienda no consumir alimentos en los escritorios de trabajos, salas de servidores (Data Center), centrales telefónicas, ni tampoco en las cercanías de impresoras, o cualquier otro activo de información, exceptuando las modalidades y/o circunstancias de trabajo que lo requieren.

7. POLÍTICA DE CLAVES DE ACCESO DE LOS SISTEMAS INFORMÁTICOS

- Las claves de sistemas de todo nivel (ej.: root, administración de servidores y bases de datos, cuentas de administración de aplicaciones, etc.) se recomienda cambiarlas al menos una vez por año.
- Las claves de usuario (ej.: correo electrónico, web, escritorio, etc.) se recomienda cambiarlas cada tres meses como mínimo.
- Las claves no deben ser enviadas por correo electrónico ni por otro tipo de formulario electrónico.
- No se debe utilizar claves débiles, como las que tienen menos de 6 caracteres, rut, nombres, etc.
- Se debe usar claves fuertes, que contengan mayúsculas y minúsculas, dígitos, por lo menos 8 caracteres.
- Las claves no deben ser escritas en papel ni almacenadas en línea. Es de responsabilidad personal cuidar de nunca compartir sus claves. Las claves deben ser tratadas como sensibles y representa información confidencial del Instituto.
- Si alguna cuenta o clave es sospechosa de estar comprometida, reportar el incidente al Encargado de Seguridad del Instituto o a su jefatura vía correo electrónico, o solicite el cambio a quien corresponda.

Se recomienda:

- No utilizar claves antiguas cuando las cambie, no revelar su clave por correo electrónico.
- No revelar su clave por teléfono a nadie, no revelar su clave al Jefe (a).
- No hablar de su clave en frente de otras personas, no revelar datos sobre la forma o estructura de sus claves.
- No revelar su clave a quien se lo pregunte ni en formularios de seguridad. No comparta claves con miembros de la familia.
- No revelar su clave a colegas cuando salga de vacaciones.

Los desarrolladores de aplicaciones deben asegurarse que en sus programas:

- Las claves deben soportar autenticación por usuario individual.
- Se deben contemplar módulos para que los usuarios cambien la clave de acceso que se les ha asignado por primera vez.
- El acceso a los sistemas deberá ser bloqueado después del tercer intento negativo, al menos por un día. Con el objeto de asegurar la continuidad de servicio, el bloqueo puede ser levantado por el administrador del sistema en menor plazo, siempre que se asegure de la identidad de quien solicita el levantamiento.
- El acceso a las redes del instituto en forma remota deben controlarse a través de un nombre de usuario y contraseña.

8. DIFUSIÓN

La política de Control de Acceso a la Información Física y Digital, sus normas, procedimientos y sus correspondientes actualizaciones y/o modificaciones, como también las resoluciones, oficios y/o circulares que emanen de la Dirección Nacional o del Encargado de Seguridad de la Información, deben ser publicados en la página de la intranet del IPS.
El encargado de Seguridad de la Información en conjunto con el Departamento de Seguridad de la Información, impulsarán un Plan de Comunicación o Sensibilización de las políticas organizacionales de la

Seguridad de la Información, además de otras acciones de comunicación y difusión por los distintos medios que posee la institución.

9. REEVALUACIÓN

La política de Control de Acceso a la Información Física y Digital, que considera la seguridad de la información y sus normas, que se aplican a los activos de información serán examinados, revisados y reevaluados por el Comité de Seguridad 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 de introducir las modificaciones apropiadas.