Junta Nacional de Jardines Infantiles
Ministerio de Educación
Gobierno de Chile

RESOLUCIÓN EXENTA N° 015/ 000016

REF.: Deja sin efecto Resolución Exenta N° 015/2492, de fecha 13 de octubre de 2011, de la Vicepresidenta Ejecutiva de la Junta Nacional de Jardines Infantiles, que "Aprueba políticas específicas de seguridad de la información"; y aprueba Manual de Políticas Específicas de seguridad de la Información.

SANTIAGO, 15 ENE 2015

VISTOS:

1°) la Ley N° 17.301, de 1970, del Ministerio de Educación, que "Crea Corporación Denominada Junta Nacional de Jardines Infantiles"; **2°)** la Ley N° 19.628, de 1999, del Ministerio Secretaria General de la Presidencia, que trata "Sobre protección de la vida privada"; **3.)** la Ley N° 20.285, de 2008, del Ministerio Secretaria General de la Presidencia; **4.)** el Decreto Supremo N° 1.574, de 1971, del Ministerio de Educación, que "Aprueba Reglamento de la Ley 17.301, que Crea la Junta Nacional de Jardines Infantiles"; **5°)** el Decreto Supremo N° 83, de 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"; **6°)** el Decreto Supremo N° 156, de 2014, del Ministerio de Educación, que "Designa en forma transitoria y provisional a doña Desirée López de Maturana como Vicepresidenta Ejecutiva de la Junta Nacional de Jardines Infantiles"; **7°)** la Resolución Exenta N° 015/2492, de 13 de octubre de 2011, de la Vicepresidenta Ejecutiva de la Junta Nacional de Jardines Infantiles, que "Aprueba políticas específicas de seguridad de la información"; **8°)** la Resolución N° 1600, de 2008, de la Contraloría General de la República, y demás antecedentes tenidos a la vista.

CONSIDERANDO:

1. Que, mediante Resolución Exenta N° 015/803, de fecha 23 de marzo de 2011, de la Vicepresidenta Ejecutiva de este Servicio, se aprobó la Política General de la Seguridad de la Información para la Junta Nacional de Jardines Infantiles.

2. Que, tal política requiere el señalamiento de normas particulares relativas, entre otras a la seguridad organizativa, a la seguridad lógica, a la seguridad física y a los aspectos jurídicos, en manejo de la información.

3. Que, debido a lo señalado en el considerando anterior, mediante Resolución Exenta N° 015/2492, de 13 de octubre de 2011, de la Vicepresidenta Ejecutiva de esta Institución, se aprobó un Manual de Políticas Específicas de Seguridad de la Información.

4. Que, a través de Memorándum N° 015/77, de fecha 20 de junio de 2014, de la Directora del Departamento de Informática (TyP), se solicita dejar sin efecto la Resolución Exenta N° 015/2492, individualizada en el considerando que antecede, y aprobar un nuevo Manual de Políticas Específicas de Seguridad de la Información, debido a la necesidad de la actualización del mismo.

5. Que, es necesario dictar el correspondiente acto administrativo, mediante el cual se aprueba el "Manual de Políticas Específicas de Seguridad de la Información", de la Junta Nacional de Jardines Infantiles.

RESUELVO

1.- APRUÉBASE el siguiente Manual de Políticas Específicas de Seguridad de la Información:

JUNTA NACIONAL DE JARDINES INFANTILES
FISCALIA

Junta Nacional de Jardines Infantiles
Marchant Pereira N° 726, Providencia
Fono (56-2) 654 50 00
www.junji.cl

Manual de Políticas Específicas de Seguridad de la Información

JUNJI
Ministerio de Educación

Gobierno de Chile

Actividad		Cargo/Función
Elaboración Modificación		Encargados Seguridad de la Información
Revisión	Técnica	Directora Subdepartamento Informática
	Normativa	Encargado Seguridad de la Información

Junta Nacional de Jardines Infantiles

CONTROL DE CAMBIOS

Versión	Fecha	Descripción de cambios
2.0	30/05/14	Documento elaborado en base al manual de políticas específicas de seguridad de la información del año 2011.

CONTENIDO

JUNTA NACIONAL DE JARDINES INFANTILES
FISCALÍA

1. OBJETIVO

El manual de políticas específicas de seguridad de la información tiene como objetivo entregar la información necesaria para que los funcionarios y funcionarias de la JUNJI puedan cumplir con la política de seguridad de la información institucional. La seguridad de la información tiene como objetivo velar por la disponibilidad, confidencialidad e integridad de la información institucional y la de los niños y familias que mantiene, dando también, conformidad con las normativas y leyes aplicables.

2. ALCANCE

Este manual está orientado a todas las funcionarias y funcionarios de la Institución, así como a personas externas a la institución que tienen acceso a los datos y recursos de la institución. Este documento contiene los lineamientos y procedimientos para dar cumplimiento a la política de seguridad de la información.

3. TERMINOLOGÍA

Información: "Datos que poseen significado". (ISO 9000:2005). "La información es un activo que, como otros activos importantes del negocio, es esencial al negocio de la organización y en consecuencia necesita ser protegido adecuadamente". (ISO/IEC 27000:2009)

Pilares de la Seguridad de la Información: La seguridad de la información se sustenta en tres pilares fundamentales.

> **Disponibilidad:** Es el atributo de la información que indica que ésta se encontrará en condiciones de ser utilizada por los usuarios autorizados, pudiendo acceder a las aplicaciones y sistemas cuando lo requieran para utilizar la información apropiada al desempeñar sus funciones.
>
> **Confidencialidad:** Es el atributo de la información, que establece que ésta se encontrará protegida de usuarios no autorizados.
>
> **Integridad:** Es el atributo de la información que permite entender que ésta se encuentra completa, actualizada y es verás, sin modificaciones inapropiadas o corrupción.

Proceso: Es un conjunto de actividades coordinadas y organizadas que se realizan con un fin determinado.

Activos de Información: Corresponden a todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.

Comité de Seguridad de la Información: Es un cuerpo integrado por representantes de todas las áreas sustantivas del Organismo, destinado a garantizar compromiso de las autoridades con las iniciativas de seguridad de la información.

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información. Postura institucional a través de la cual se busca proteger los conocimientos que mantiene el Servicio, en el desempeño de sus funciones, mediante la gestión de dicha información, particularmente sus comunicaciones, bases de datos y actos administrativos, con el propósito de asegurar la continuidad de los procesos institucionales.

Evento de seguridad de la información: "ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de

JUNTA NACIONAL DE JARDINES INFANTILES
FISCALÍA

información o la falla de salvaguardas, o una situación previamente desconocida que pueda ser pertinente a la seguridad" (NCh-ISO 27002).

Incidente de seguridad de la información: "un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información" (NCh-ISO 27002).

Debilidad de seguridad de la información: Es una condición o característica institucional que permitiría, eventualmente, la ocurrencia de un incidente de seguridad de la información.

Norma Chilena Oficial ISO 27002 (NCh-ISO 27002): Norma chilena que corresponde con la norma internacional ISO/IEC 27002 que contiene el código de prácticas para la gestión de seguridad de la información. La serie de normas ISO/IEC 27000 contiene las mejores prácticas recomendadas en seguridad de la información en el contexto de un sistema de gestión de seguridad de la información (SGSI).

Sistemas: Se refiere a los sistemas informáticos o metodológicos que utiliza la institución para procesar la información. Estos sistemas pueden ser solo de uso interno, o también de uso externo, que incluye a los usuarios/clientes/beneficiarios u otros organismos públicos y privados.

Infraestructura: Es la base física que soporta sistemas, equipamiento y la información en sí. Incluye edificios, salas, cableado, muebles, contenedores, bodegas, y otros.

4. DOCUMENTOS APLICABLES O RELACIONADOS

- Política de Seguridad de la Información.
- Política Específica Control de Acceso.
- Política Específica Continuidad de Negocio.
- Manual de Operaciones
- Decreto Supremo n° 83 de 2004
- Norma internacional ISO/IEC 27000
- Ley 19.628, de 1999, sobre protección de datos de carácter personal
- Ley 20.285, de 2008, sobre acceso a la información pública

JUNTA NACIONAL DE JARDINES INFANTILES
FISCALÍA

5. INTRODUCCIÓN

La Junta Nacional de Jardines Infantiles tiene como misión entregar Educación Parvularia de calidad preferentemente a niños y niñas en situación de vulnerabilidad social para contribuir con el desarrollo educativo integral de la primera infancia. Para esto, y considerando que se trata de una entidad pública, la información siempre ha sido un activo de gran valor para la institución, en cuanto es la base para gestionar recursos, identificar necesidades y entregar conocimiento y comunicación a los funcionarios, los párvulos/as, sus familias y otras entidades externas.

Considerando la diversidad de información crítica en JUNJI, como los datos de los funcionarios, sus remuneraciones, datos de jardines propios y operados por terceros, datos de presupuesto institucional y su contabilidad, datos secretos como sumarios, datos protegidos como la información del párvulo y sus familias, es que se vuelve sumamente relevante proteger toda la información institucional. Es por esto que el estado ha resuelto generar un sistema de seguridad de la información en todas las instituciones públicas.

Este sistema de seguridad de la información se puede definir como un conjunto de políticas, procedimientos, y mecanismos que eviten el daño, la pérdida y la fuga de la información institucional y de la información que emite o utiliza desde o hacia entidades externas.

La seguridad de la información no es un asunto que solo implique informática, ya que también involucra en gran medida a la alta dirección, el área jurídica, recursos humanos, recursos físicos y financieros y a todos y cada uno de las personas que se desempeñan en la institución ya que todos tenemos algún grado de acceso a esta.

6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad de la información es la directriz principal de la organización, debe estar alineada con la misión y los objetivos de la institución y cualquier otra política, procedimiento o mecanismo implementado en JUNJI deben estar alineados con esta. Esta política, como cualquier otra, debe ser conocida por todas las personas que pertenecen o trabajan con JUNJI.

Los elementos principales de la política de seguridad de la información se describen a continuación

6.1. DECLARACIÓN INSTITUCIONAL

La Junta Nacional de Jardines Infantiles expresa su compromiso con la gestión de la Seguridad de la Información, entendiendo que este mecanismo asegurará una correcta continuidad del Servicio, permitiendo cumplir en todo momento los objetivos institucionales.

JUNTA NACIONAL DE JARDINES INFANTILES
FISCALÍA

6.2. PRINCIPIOS RECTORES DE LA SEGURIDAD DE LA INFORMACIÓN

1. El desafío institucional es proteger la información del Servicio contra amenazas que atentan contra el valor, la imagen y la continuidad institucional mediante el resguardo y administración de los activos de información.

2. Para ello la JUNJI reconoce la necesidad de establecer una cultura institucional concientizando, formando y capacitando a todos y todas los/las funcionarios/as en las materias de seguridad de la información.

3. Identificar las vulnerabilidades y amenazas asociadas a los activos de información con el procedimiento de gestión de riesgos institucional.

4. Establecer directrices específicas y procedimientos que permitan proteger la integridad, disponibilidad y confidencialidad de los activos de información de las amenazas y vulnerabilidades internas y externas.

5. Establecer los mecanismos necesarios para controlar la implementación de políticas, procedimientos y planes de seguridad de la información.

6. Establecer directrices específicas y planes que permitan recuperar y restaurar los activos de información que sufrieron algún incidente, garantizando el nivel apropiado de disponibilidad de servicios y procesos.

7. Cumplir con las normativas legales, regulatorias, contractuales y técnicas en temas de seguridad de la información.

8. Hacer efectiva la responsabilidad administrativa de los funcionarios que violen la política de seguridad de la información y/o la normativa asociada.

6.3. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

La/El Vicepresidenta conforma, mediante resolución, al Comité de Seguridad de la Información. Su rol clave es gestionar la política de seguridad de la información, reuniendo la representación y presencia de los distintos departamentos y unidades de la JUNJI. Sus tareas específicas son:

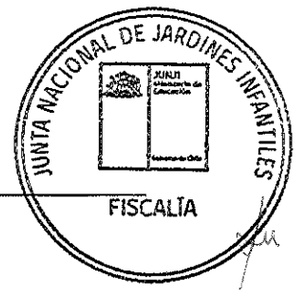
- Proponer estrategias y soluciones específicas para el establecimiento de los controles necesarios para implementar las políticas de seguridad establecidas y la debida solución de las situaciones de riesgos detectadas.

- Evaluar la efectividad de la implementación de procedimientos específicos y estándares que se desprenden de las políticas de seguridad de la información.

- Arbitrar conflictos en materia de seguridad de la información y los riesgos asociados, y proponer soluciones.

- Coordinar su actuar con los Comités de Calidad y de Riesgos de la Institución, para mantener alineadas las estrategias comunes de gestión.

- Reportar, en conjunto con el Encargado de Seguridad, a la jefatura del Servicio, respecto de oportunidades de mejora en la Gestión de la Seguridad de la Información, así como de los incidentes relevantes y su posible solución.



7. BASES NORMATIVAS Y JURIDICAS

El decreto supremo número 83 del 2004 es el marco legal que impone el desarrollo de un SSI. Este se basa técnicamente en la norma chilena NCh2777 la cual es derogada por la nueva NCh27002. (MINSEGPRES)

El 2010, 2011 y 2012 a nuestro servicio se incorpora el PMG-SSI el cual busca implementar un sistema basado en los controles de la NCh27002, para apoyar al cumplimiento del DS n°83. La familia de normas internacionales ISO/IEC 27000 presentan un sistema de gestión de la seguridad de la información.

El estatuto administrativo también hace referencia a los aspectos de seguridad de la información, como en el artículo 61, punto h: "Guardar secreto en los asuntos que revistan el carácter de reservados en virtud de la ley, del reglamento, de su naturaleza o por instrucciones especiales".

La ley 19.628, de 1999 sobre protección de datos de carácter personal que dispone sobre el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares.

La Ley 20.285, de 2008, sobre acceso a la información pública

8. POLÍTICAS ESPECÍFICAS

El objetivo de este capítulo es proporcionar la información necesaria a los usuarios/as y funcionarios/as de la Junta Nacional de Jardines Infantiles, relativas a las normas y mecanismos que deben cumplir y utilizar para dar cumplimiento a la política de seguridad de la información.

8.1. POLÍTICAS PARA TODO FUNCIONARIO/A JUNJI Y PERSONAS EXTERNAS

1. **Todo funcionario de informarse sobre los temas de seguridad de información** dentro de las funciones de su cargo y toda otra información institucional a la cual tienen acceso, por ejemplo:

    a) Los funcionarios deben leer el estatuto administrativo. Contiene los derechos y deberes sobre la información confidencial, personal y sumarios administrativos, entre otros.

    b) La ley 19.628 trata sobre protección de datos de carácter personal.

    c) La ley 17.336 trata sobre propiedad intelectual y derecho de autor.

2. **La información institucional** procesada, manipulada o almacenada por el/la funcionario/a es propiedad exclusiva de la Junta Nacional de Jardines Infantiles.

    a) Los datos de correo electrónico u otra información protegida por datos de acceso puede ser accesada por terceros solo en el caso de un sumario administrativo o que una autoridad jurídica así lo dictamine.

    b) Ningún funcionario debe entregar información institucional a terceros. El intercambio de información con terceros debe estar institucionalmente formalizada mediante una solicitud de acceso a información pública o mediante un convenio firmado por la alta dirección.

    c) La información institucional oficial la entrega una entidad designada formalmente mediante un informe. No utilizar cualquier dato entregado por bases de datos o funcionarios que tengan acceso a estos.

JUNTA NACIONAL DE JARDINES INFANTILES
FISCALÍA

d) Para la información en papel y/o documentos electrónicos siga los procedimientos de gestión documental establecidos en la unidad en que se desempeña.

3. **Los servicios de la red de datos institucional** son de exclusivo uso institucional y para dar respuesta a los distintos procesos administrativos de las distintas áreas de negocio de la JUNJI.

   a) Queda expresamente prohibido utilizar estos recursos para fines distintos al mencionado, esto incluye, por ejemplo, guardar o consumir contenido multimedia, utilizar redes sociales, llamadas telefónicas inapropiadas, descargar y compartir contenido que no corresponda a las funciones institucionales.

   b) El Comité de Seguridad de la Información, se reserva el derecho de monitorear el uso de la red del usuario, pudiendo limitar el acceso de este usuario a estos recursos.

   c) El acceso a internet se encuentra limitado para evitar que los usuarios accedan accidentalmente a contenido perjudicial para la seguridad de la información. Si el usuario encuentra que este filtro no permite desempeñar las tareas que le corresponden a su función institucional, debe comunicarse con el encargado de Redes de informática para comunicárselo. En caso de que el encargado de Redes de informática identifique que este acceso es potencialmente perjudicial, debe derivarse el caso al comité de seguridad de la información para su resolución.

   d) Los funcionarios de la unidad de comunicación, el jefe/a de gabinete, los Directores/as Regionales, y la/el vicepresidenta/e ejecutiva/o podrán tener acceso internet a contenido multimedia, redes sociales y similares. Cualquier otro caso debe ser revisado y resuelto por el comité de seguridad de la información.

   e) La conexión de dispositivos personales a la red de datos solo debe ser con el objeto de apoyar las funciones institucionales.

4. **La red eléctrica** es el sustento de la red de datos y servicios de información institucionales.

   a) No utilice hervidores eléctricos, máquinas de café, tostadoras, hornos y similares en la oficina.

   b) No utilice calefacción ni ventilación eléctrica personal o no autorizada en la oficina.

   c) Cuide el cableado eléctrico y enchufes con el fin de evitar cortocircuitos.

   d) No recargue la red eléctrica utilizando alargadores y múltiples (zapatilla eléctrica).

5. **El acceso a la red de datos institucional** se otorga de forma a cada administrativo de JUNJI en donde se identifica de forma única e inequívoca. Los datos de acceso (usuario y contraseña) son de uso personal e intransferible, por lo que cualquier acción registrada bajo su nombre no podrá ser negada ni repudiada.

6. **Los datos de acceso (usuario y contraseña)** son de uso personal e intransferible. La contraseña y los mecanismos asociados a estas deben cumplir:

   a) Cuando a un usuario se le otorga una cuenta esta tiene una contraseña inicial, la cual debe cambiarse inmediatamente.

JUNTA NACIONAL DE JARDINES INFANTILES
FISCALÍA

b) Ningún funcionario de informática tiene acceso a las contraseñas de usuario ya que estas se almacenan de forma encriptada. Si olvidó su contraseña, debe solicitar su restablecimiento de forma escrita a soporte informatica@junji.cl, o al administrador del sistema que corresponda. Luego debe cambiarse inmediatamente.

c) Cuando deje un rol en un sistema de información pida que revoquen sus privilegios de acceso. Nadie puede entrar con ellos en su ausencia.

d) Si guarda sus contraseñas en papel guárdelo bajo llave. Si guarda sus contraseñas en un documento digital cerciórese que solo usted tiene acceso al archivo. No escriba las contraseñas en post-it o similares.

e) No establecer contraseñas simples relacionadas con alguna característica de su persona o relacionado con su vida o la de parientes, como nombres de hijos o mascotas u otros parientes, dirección o número de vivienda, ídolos, palabras relacionadas con hobbies, deportes, fechas de cumpleaños o alguna otra fecha importante.

f) No use palabras simples que puedan aparecer en un diccionario (todos los idiomas).

g) No utilice las mismas contraseñas que utiliza en servicios externos a JUNJI. Como la de correo electrónico personal o redes sociales.

h) No utilice contraseñas numéricas simples y/o repetitivas ni enumeraciones como: 1234, 123456, 0000, 000000, 1111, 111111, 4321, 654321, 7777, 777777, abcd, abcde, qwer, qwerty, asdf, asdfgh, zxcv, zxcvbn, poiu, poiuyt, lkjh, lkjhgf, ñlkj, mnbv, mnbvcx, aeiou, uoiea, zyxw, zyxwvu, etc.

i) No utilice frases de uso común, significativas, nombre del servicio o sistema, o con letras cambiadas con números como: micontraseña, mi contraseña, iloveyou, i love you, te quiero, tequiero, contr@señ@, c0nt4s3ñ@, p@ssw0rd, t3qu13r0, t3 qu13r0, buenos días, buenas noches, ábrete sésamo, ábrete sésamo, entra, clave, ábrete, computador, abaco, sigfe, facebook, rrhh, recursos humanos, SisTrans, soy el mejor, te odio, teodio, ihateyou, i hate you, dios me ama, diosmeama, Windows, computador, Windows 7, correo electrónico, correo, email, JUNJI, jardines infantiles, jardinesinfantiles, jardininfantil, emailjunji, emailjunji, correo junji, red junji, etc.

j) Una contraseña apropiada combina letras mayúsculas, minúsculas, números y signos y tiene al menos 6 caracteres. Ejemplos de contraseñas apropiadas son "Os540.tém-8", "wyq_55.g8L", etc.

7. **El servicio de correo electrónico** de la Junta Nacional de Jardines Infantiles es un servicio institucional, el cual se presta a los funcionarios/as y servidores a honorarios creados como usuarios de la red. El objetivo del correo institucional es ser un medio de comunicación oficial electrónico. Se debe hacer uso de él según su objetivo y acatando todas las disposiciones de seguridad diseñadas para su utilización y evitar el uso o introducción de software malicioso a la red institucional.

   a) No se crearán cuentas de correo genéricas, sin previa consulta y resolución del Comité de Seguridad de la Información.

   b) El usuario será responsable de cualquier información que sea enviada a través de su cuenta de correo institucional, la única excepción serán hechos comprobables de violaciones de seguridad electrónica.

JUNTA NACIONAL DE JARDINES INFANTILES
FISCALÍA

c) El Comité de Seguridad de la Información, se reserva el derecho de monitorear las cuentas de usuarios, que presenten un comportamiento que, eventualmente, afecte la seguridad de la red institucional.

8. **La seguridad de los activos de información,** como computadores, documentos en papel, dispositivos móviles, muebles con documentos y equipos, son de responsabilidad de su usuario, pero también todo funcionario debe velar por la seguridad de los activos de su entorno.

   a) Para dar resguardo a la información digital no sistematizada se aconseja utilizar las "carpetas compartidas" que otorga el departamento de informática, ya que se respaldan una vez a la semana. Para más seguridad, mantener copias en la "carpeta compartida" y en el almacenamiento local del equipo (disco duro del computador).

   b) Cuando un funcionario entrega un computador o dispositivo personal debe solicitar que se formatee o elimine su información antes de entregarlo a terceros y después de recuperar la información relevante.

   c) No instalar software o guardar archivos que no tengan que ver con su función institucional, como reproductores de videos y películas.

   d) Mantener la pantalla de computador o dispositivos móviles bloqueada y con contraseña. Por ejemplo, al levantarse de su escritorio, el funcionario siempre debe presionar "teclaWindows+L" en el teclado para bloquear la pantalla del computador.

   e) Mantener los activos de información de su entorno salvo de filtraciones de agua, descargas eléctricas, caídas desde alturas, fuego, explosiones, robos y atentados.

   f) No permitir que los activos de información sean retirados sin las autorizaciones correspondientes. Verificar que estos activos no contengan información que no deba retirarse. Por ejemplo, al dar de baja algún mueble, verificar que no contenga documentos.

   g) Los documentos en papel eliminados (solo se pueden eliminar copias, o documentación no oficial) deben ser triturados o rasgados al eliminarse, en especial aquellos que tengan información personal.

   h) El equipamiento y su configuración no debe ser manipulado por funcionarios/as que no tengan la competencia ni autorización necesaria.

   i) Los funcionarios no deben utilizar medios de almacenamiento removible (por ejemplo pendrive) de carácter personal en el desempeño de sus labores. Es bien conocido que es una de las principales fuentes de ataques de virus y software malicioso en general. Es por esto que es necesario que los funcionarios no mezclen este tipo de dispositivos en la oficina y, por ejemplo, su hogar o amistades. Se recomienda solicitar pendrives para la unidad con su propio presupuesto, y utilizarlos solo en el ambiente de oficinas.

   j) Evitar, dentro de lo posible, el transporte de dispositivos portátiles, con el fin de evitar pérdidas y robos.

9. **El acceso de terceros** a cualquier activo de información debe incluir cláusulas de seguridad de la información en los contratos correspondientes. Estas cláusulas son mantenidas por el área jurídica, según la resolución exenta nº 015/2918 del 2018 "Aprueba Instrumento de confidencialidad de la Información". El cual contiene el convenio de confidencialidad para que el adjudicatario y quienes participen guarden absoluta confidencialidad sobre la información que se les proporcione.

JUNJI NACIONAL DE JARDINES INFANTILES
FISCALÍA

10. **El acceso de visitas** en las dependencias, ya sean personales o administrativas, deben limitarse en lo posible a la recepción y salas de reuniones.

11. **La responsabilidad sobre los activos de información** depende de la clasificación de estos. Los activos pueden dividirse en 3 categorías o niveles:

    a) **Información en Sí.** La información es responsabilidad de la unidad o departamento que la origina y/o mantiene, por ejemplo, los datos de los funcionarios/as es responsabilidad de Recursos Humanos y los datos de contabilidad son responsabilidad de Recursos Financieros.

    b) **Equipos, Infraestructura o Medios asociados a la información.** En grandes rasgos:

        i. Los equipos digitales, red de datos y telefonía IP son de responsabilidad del área de informática.

        ii. La infraestructura eléctrica y estructural son responsabilidad del departamento de cobertura e infraestructura.

        iii. La seguridad perimetral de control de acceso a las dependencias (guardias de seguridad) es de responsabilidad de servicios generales (Recursos Físicos).

        iv. Todo funcionario es también parte responsable sobre los activos que utiliza, como computadores, impresoras y medios removibles.

    c) **Las personas que producen o utilizan esta información.** Todo funcionario/a que tiene acceso a los activos de información institucionales es responsable de conocer las normas de seguridad de la información y las leyes de propiedad intelectual y de la reserva de información personal.

        i. La venta, intercambio y reproducción de cualquier material audiovisual (películas, música, libros) con derechos de autor queda expresamente prohibido si no se poseen los permisos adecuados.

        ii. La información de personas que maneja la institución es de naturaleza reservada. Incluye datos de los niños, sus familias, los datos de los funcionarios y cualquier otro dato personal de cualquier procedencia, como entidades externas. La información personal no puede ser publicada, ni comunicada a entidades externas sin el consentimiento de las personas a las cuales pertenecen estos datos. Solo los funcionarios cuya función institucional implique el uso o recolección de datos personales pueden tener acceso a estos.

        iii. El funcionario/a que produce o modifica algún tipo de información debe siempre propender a la integridad, completitud y oportunidad de esta.

12. **La obligación de informar** cualquier hecho que pueda comprometer la seguridad de la información aplica a todos los funcionarios de la Junta Nacional de Jardines Infantiles.

    a) Debe informar al encargado del área respectiva, si este funcionario/a no puede dar la solución apropiada, o si es de impacto transversal a la institución, informar al comité de seguridad de la información al correo csi@junji.cl o mediante memorándum.

JUNTA NACIONAL DE JARDINES INFANTILES
FISCALÍA

b) Debe informar debilidades que puedan atentar contra la seguridad de la información. No es necesario esperar a que ocurra un incidente para darlo a conocer.

c) Debe informar cualquier incidente que viole las políticas de seguridad de la información.

d) Ejemplos de hechos para informar:

i. Informar la presencia de un desconocido en las dependencias a los guardias de seguridad o encargado de la unidad.

ii. Informar la fuga de información de carácter personal (niños y sus familias) al comité de seguridad de información o encargado de la unidad.

iii. Informar un posible foco de incendio por cortocircuito, al área de servicios generales e infraestructura.

iv. Informar un posible corte de los cables de datos de la red al encargado de informática.

8.2. POLÍTICAS RELATIVAS A UNIDADES ORGANIZATIVAS Y SUS REPECTIVOS ENCARGADOS

1. **Cada vez que un funcionario se integre** a una unidad (sección, subdirección, departamento), el encargado de esa unidad debe:

a) Informar a soporte informática para crear al usuario en la red institucional. El encargado del área debe informar de forma oportuna la creación del usuario en la red institucional. Esta petición se realiza mediante el llenado de un formulario que debe ser solicitado y enviado al área de informática, específicamente al área soporte (soporte_informatica@junji.cl). Si por cualquier razón el usuario no llega a integrarse a la unidad, debe ser informado para que informática cancele la creación o revoque los privilegios creados para ese usuario.

b) En la inducción de este nuevo funcionario indicar las políticas de seguridad de información dándole acceso a este documento. Esta inducción debiera realizarse antes de entregarle cualquier activo de información.

c) Entregarle los privilegios necesarios en los sistemas que este encargado administra o de los cuales es responsable.

d) Si el funcionario proviene de otra unidad JUNJI, identificar los sistemas en donde el usuario tenía privilegios y contactar con los administradores de estos para revocarle los privilegios que correspondan.

2. **Cada vez que un funcionario se desligue** de una unidad (sección, subdirección, departamento), el encargado de esa unidad debe:

a) Revocar los privilegios en los sistemas que este encargado administra o de los cuales es responsable.

b) Verificar que la persona no se lleve ningún activo de información institucional con ella. Esto implica equipos (teléfono, impresoras, computador, unidades de almacenamiento de datos removible), muebles que puedan almacenar información y documentos en sí que correspondan a la unidad. La única excepción es cuando el funcionario queda dentro de la institución (cambio de unidad), en este caso el usuario puede quedar con el teléfono,

JUNTA NACIONAL DE JARDINES INFANTILES
FISCALÍA

computador, muebles, medios removibles y documentos que no correspondan al dominio de la unidad. Si se lleva consigo muebles, computador, o medios removibles verificar que la información almacenada en estos activos quede a disponibilidad de la unidad cuando corresponda. Debe indicar a la unidad de inventario cualquier movimiento de muebles y equipo.

c) Informar de forma escrita a informática para que se elimine el acceso a la red institucional. Este proceso es obligatorio, la única excepción es cuando el funcionario queda dentro de la institución (cambio de unidad).

3. **Los sistemas de información** que pertenecen al dominio de la unidad, son responsabilidad de esa unidad en cuanto a la información que maneja y a su administración. Mientras el encargado de una unidad es responsable de estos aspectos del sistema, el administrador del sistema puede ser cualquier otro funcionario de la unidad. El área de informática solo es el responsable del aspecto técnico de estos sistemas, es decir, su disponibilidad en la red, instalación o desinstalación, mantención de las maquinas correspondientes, sistema operativo y bases de datos.

   a) **Los respaldos** de la información de estos sistemas, incluyendo las "carpetas compartidas" que se utilicen, deben ser solicitadas explícitamente de forma escrita al encargado/a de informática, indicando específicamente qué se debe respaldar y con qué periodicidad.

   b) **Los privilegios de los usuarios** de los sistemas que la unidad administre deben ser revisados con una periodicidad al menos anual. Cada usuario debe tener los privilegios mínimos necesarios para poder realizar su labor institucional.

   c) **Todos los usuarios de los sistemas deben tener la capacitación o inducción** necesaria para utilizar de forma correcta los sistemas de información. Esto incluye directivas sobre archivos y carpetas compartidas. Esto con el fin de evitar la pérdida, fuga o daño de la información.

   d) **Todo sistema de información debe contar con las medidas mínimas** de seguridad de la información:

      i. Los usuarios son identificados de forma individual, inequívoca y certera, de tal forma que estos usuarios no podrán negar ninguna acción registrada a su nombre.

      ii. Todo cambio en los datos debe ser registrado junto al nombre de quien dispara esta acción.

      iii. Las contraseñas se guardan de forma encriptada.

      iv. Los sistemas de acceso masivo deben tener un sistema de recuperación de contraseña automático confidencial y seguro.

      v. Los privilegios para ver, crear, modificar y eliminar pueden ser administrados y están adecuadamente otorgados a los usuarios que corresponde.

      vi. Toda creación, modificación o eliminación de cualquier registro debe incluir al usuario que la realiza.

      vii. El sistema no puede estar disponible a través de internet sin antes ser revisada su seguridad técnica, administrativa y autorizado por el comité de seguridad de la información.

JUNTA NACIONAL DE JARDINES INFANTILES
FISCALÍA

viii. El sistema es respaldado según lo requerido.

ix. El manual de usuario existe y es conocido.

x. Se han tomado las medidas necesarias para asegurar la integridad de la información tratada en el sistema y las medidas de los puntos anteriores. Esto se corrobora usualmente con un informe de pruebas y validaciones del sistema durante su desarrollo e implementación.

e) **El mantenimiento estándar** de los sistemas de parte de informática son los siguientes:

i. Respaldo según las directivas solicitadas por la unidad responsable

ii. Mantenimiento sistema operativo

iii. Mantenimiento a bases de datos

iv. Mantenimiento espacio de almacenamiento

v. Mantenimiento de Hardware

vi. Pruebas de recuperación

Cualquier otro requerimiento específico para la mantención del sistema debe ser solicitado explícitamente al encargado/a de informática de forma escrita.

f) **Los cambios que deben realizarse al sistema para adaptarse a los cambios** del negocio deben solicitarse con la anticipación necesaria con el fin de disponer con los recursos necesarios en la fecha que los cambios ocurran.

i. El periodo adecuado para solicitar y planificar mejoras, nuevos módulos o nuevos sistemas de información es antes o durante la planificación presupuestaria del año anterior.

ii. Siempre deben solicitarse las medidas de seguridad de información mínimas y específicas en toda mejora, nuevos módulos o nuevos sistemas, según la relevancia y confidencialidad de la información tratada.

iii. Toda mejora o desarrollo de nuevos módulos debe realizarse en un ambiente de desarrollo controlado, sin acceso a los datos oficiales. Si se trata de información confidencial esta información no debe ser una copia de los datos reales. Lo mismo aplica para las pruebas y validaciones. Esto con el fin de resguardar los datos oficiales de posibles errores de sistema y acceso de terceros.

4. **Mantener siempre a mano los números y canales de emergencia,** y cerciorar que también lo hagan los funcionarios del área a cargo. La detección temprana de un incidente puede salvar a los funcionarios y activos de información.

5. **La información contenida en documentos en papel o digitales** debe ser gestionada adecuadamente. El encargado de una unidad debe establecer y mantener la gestión sobre la documentación en papel y digital no sistematizada. Para esto utilizar los principios de gestión documental de la sección de gestión de calidad.

a) Los documentos originales oficiales no deben eliminarse bajo ningún concepto. Las excepciones son autorizaciones directas de la presidencia de la república. Las copias pueden ser eliminadas.

JUNTA NACIONAL DE JARDINES INFANTILES
FISCALÍA

b) Los documentos en papel deben almacenarse bajo condiciones favorables. lejos de la humedad, filtraciones agua lluvia, fuentes de calor, llamas, equipo eléctrico, entre otros. Si es necesario, almacenar en contenedores resistentes a incendios, robos, atentados e inundaciones.

6. **Los equipos de la unidad** deben tener una mantención apropiada, y ser reabastecidos periódicamente.

   a) Si se detecta que no existe mantención en un equipo solicitarlo a la unidad correspondiente. No espere que un equipo necesario para realizar su trabajo falle cuando más lo necesita.

   b) No permita que funcionarios sin los conocimientos necesarios trate de arreglar el equipo con falla.

7. **Cualquier intercambio de información** con entidades externas a la institución debe tener asociado un convenio o acuerdo de intercambio con su debido acto administrativo. La única excepción es una solicitud de acceso a información pública con su debido procedimiento.

8. **Mantener un plan de contingencia** frente a fallas técnicas. Los incidentes de seguridad ocurren incluso con los estándares más altos de seguridad, es por esto que debe mantenerse un plan en caso de falla de los sistemas y canales principales de comunicación e información, según el nivel de criticidad del proceso en la JUNJI. Revisar la Política de Continuidad de Negocio para más detalles.

8.3. POLÍTICAS RELATIVAS A LA ALTA DIRECCIÓN

1. **La organización interna en torno a seguridad de la información** debe ser instaurada a nivel institucional:

   a) Establecer u marco para iniciar y controlar la seguridad de la información.

   b) Buscar el asesoramiento necesario para instaurar un sistema de seguridad de la información.

   c) Establecer las responsabilidades necesarias.

   d) Asegurar que los objetivos de seguridad de la información son identificados y cumplen los lineamientos de la organización

   e) Asegurar que los procesos de seguridad de la información se integren con los procesos ya instaurados en la organización

   f) Formular, aprobar y publicar la política de seguridad de la información institucional.

   g) Proveer los recursos necesarios para el sistema de seguridad de la información

   h) Velar por la concientización de seguridad de la información mediante comunicación interna y capacitaciones

   i) Asegurar que se aplican los controles de seguridad de la información en toda la organización.

   j) Establecer revisiones de alta dirección al estado de seguridad de la información

2. **La imagen de la JUNJI** podría verse afectada por los incidentes de seguridad de la información, por lo que se debe:

    a) Asegurar que existen y se aplican procedimientos de aspectos legales y de comunicación externa en el caso de incidentes de seguridad de la información

    b) Mantener comunicación permanente con las entidades externas que puedan auxiliar o verse afectadas por incidentes de seguridad de la información.

    c) Mantener y revisar los acuerdos de confidencialidad que se deben suscribir con entidades externas.

    d) Mantener contacto con grupos de conocimiento experto y afín en seguridad de la información.

    e) Exigir normas y estándares de seguridad de la información a proveedores que corresponda.

8.4. POLÍTICAS PARA AUDITORIAS

1. **Las auditorias son necesarias** para el sistema de seguridad de la información. Tener en cuenta lo siguiente:

    a) Se debe efectuar una auditoria de seguridad de la información con periodicidad al menos anual.

    b) La auditoría debe ser realizada por un experto en la materia de seguridad de la información y administrada por la sección de auditoría interna.

    c) Cualquier acción que amerite la ejecución de una auditoria a los sistemas informáticos deberá ser documentada y establecida su aplicabilidad y objetivos de la misma, así como razones para su ejecución, personal involucrado en la misma y sistemas implicados.

    d) La auditoría no deberá modificar en ningún momento el sistema de archivos de los sistemas implicados, en caso de haber necesidad de modificar algunos, se deberá hacer un respaldo formal del sistema o sus archivos.

    e) Las herramientas utilizadas para la auditoria deberán estar separadas de los sistemas de producción y en ningún momento estas quedarán al alcance de personal ajeno a la elaboración de la auditoría.

Junta Nacional de Jardines Infantiles
Ministerio de Educación
Gobierno de Chile

2.- DIFÚNDASE la presente resolución a todos los funcionarios de la Junta Nacional de Jardines Infantiles.

3.- DÉJASE sin efecto la Resolución Exenta N° 015/2492, de 13 de octubre de 2011, de la Vicepresidenta Ejecutiva de la Junta Nacional de Jardines Infantiles, que "Aprueba políticas específicas de seguridad de la información", por las razones indicadas en los considerandos de la presente Resolución.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

JUNTA NACIONAL DE JARDINES INFANTILES
VICEPRESIDENTA EJECUTIVA

DESTRÉE LÓPEZ DE MATURANA L.
VICEPRESIDENTA EJECUTIVA (TyP)
JUNTA NACIONAL DE JARDINES INFANTILES

JUNTA NACIONAL DE JARDINES INFANTILES
DEPARTAMENTO DE FISCALÍA

DLdeML/MCM/SMV/FRH/ERC/frc
DISTRIBUCIÓN:
-Vicepresidenta Ejecutiva
- Directores (as) Regionales I a XV Región
- Asesorías Jurídicas Regionales I a XV Región
- Departamentos DIRNAC
- Subdepartamentos DIRNAC
- Archivo Fiscalía (602/2014)