Junta Nacional de Jardines Infantiles
Ministerio de Educación
Gobierno de Chile

RESOLUCION EXENTA N° 015 / 0714

REF: Deja sin efecto Resolución Exenta N° 015/ 00688, de fecha 2 de noviembre de 2016, de la Vicepresidenta Ejecutiva de la Junta Nacional de Jardines Infantiles, que "Aprueba el Manual de Políticas Específicas de Seguridad de la Información en su Tercera Versión"; y Aprueba Manual de Políticas Específicas de Seguridad de la Información, en su Cuarta Versión.

SANTIAGO: 04 DIC 2017

VISTOS:

1°) lo dispuesto en la Ley N° 17.301, de 1970, del Ministerio de Educación Pública, que "Crea Corporación Denominada Junta Nacional de Jardines Infantiles"; **2°)** el Decreto con Fuerza de Ley Nº 1-19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que "Fija texto refundido, coordinado y sistematizado de la Ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado"; **3°)** el Decreto Supremo Nº 1.574, de 1971, del Ministerio de Educación Pública, que "Aprueba Reglamento de la Ley N° 17.301, que Crea la Junta Nacional de Jardines Infantiles"; **4°)** el Decreto Supremo Nº 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; **5°)** el Decreto Supremo N° 98, del Ministerio de Educación, de 2015; **6°)** el Memorándum N°015/431 de fecha 17 de noviembre de 2017, emanado del Director del Departamento de Planificación y Encargado Nacional de Seguridad de la Junta Nacional de Jardines Infantiles, dirigido al Director del Departamento de Fiscalía y Asesoría Jurídica; **7°)** la Resolución N° 1.600, de 2008, de la Contraloría General de la República, que "Fija Normas Sobre Exención del Trámite de Toma de Razón"; y demás antecedentes tenidos a la vista.

CONSIDERANDO:

1°) Que, mediante Resolución Exenta N° 015/00688 de fecha 2 de noviembre de 2016, la Vicepresidenta Ejecutiva de este Servicio aprobó el Manual de Políticas Específicas de Seguridad de la Información para la Junta Nacional de Jardines Infantiles, en su Tercera Versión.

2°) Que, tal Manual ha sido revisado y actualizado por el Comité de Seguridad de la Información, conforme a las nuevas necesidades de Seguridad de Información del Servicio y el cumplimiento del Programa de Mejoramiento de la Gestión 2017.

3°) Que, en este sentido se ha estimado necesario, implementar, mantener y mejorar de manera continua el Sistema de Gestión Seguridad de la Información, acotando el campo de aplicación de la NCh-ISO 27001.Of2013, a los productos estratégicos institucionales y sus subproductos. Para ello, la Junta Nacional de Jardines Infantiles ha definido el contexto y como alcance de aplicación de dicho sistema, al subproceso de Gestión de Datos de Párvulos, ejecutado geográficamente en las dependencias de la Dirección Nacional de JUNJI, el cual se asocia directamente con el producto estratégico: Educación Parvularia de Calidad, cuyo presupuesto alcanza el 99.09% del presupuesto institucional.

JUNTA NACIONAL DE JARDINES INFANTILES
FISCALÍA

4°) Que, por tal motivo, 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, en su Cuarta Versión.

RESUELVO:

1° DÉJASE sin efecto lo dispuesto en la Resolución Exenta N° 015/00688 del 2 de noviembre de 2016, de la Vicepresidenta Ejecutiva de este Servicio, que aprobó el Manual de Políticas Específicas de Seguridad de la Información de la Junta Nacional de Jardines Infantiles en su Tercera Versión, por cuanto será reemplazado por el nuevo Manual que se aprueba mediante el presente acto administrativo.

2° APRUÉBASE el Manual de Políticas Específicas de Seguridad de la Información de la Junta Nacional de Jardines Infantiles, en su Cuarta Versión, cuyo texto es el siguiente:

Junta Nacional de Jardines Infantiles
Ministerio de Educación
Gobierno de Chile

Manual de Políticas Específicas de Seguridad de la Información

Versión 4

CONTROL DE CAMBIOS	
Fecha :	14-11-2017
Elaboración/Modificación	Comité de Seguridad de la Información
Versión	**Descripción de cambios**
4	Este documento modifica, reemplaza y deja sin efecto el Manual de Políticas Específicas de Seguridad de la Información versión 3.0 aprobado según Resolución Exenta N° 015/00688 del 02-11-2016.

JUNTA NACIONAL DE JARDINES INFANTILES
FISCALÍA

Junta Nacional de Jardines Infantiles-JUNJI
Marchant Pereira 726, Providencia,
Santiago, Chile Fono: (56-2) 6545000
www.junji.cl

CONTENIDO

1. DECLARACIÓN INSTITUCIONAL

La Junta Nacional de Jardines Infantiles –JUNJI– tiene como misión otorgar educación parvularia pública, gratuita y de calidad, y bienestar integral a niños y niñas preferentemente menores de cuatro años, priorizando en aquellos que provienen de familias que requieren mayores aportes del Estado tendiendo a la universalización, a través de diversos programas educativos con una perspectiva de territorialidad; desde una visión de sociedad inclusiva y de niños y niñas como sujetos de derechos; y que reconoce las potencialidades educativas de sus contextos familiares, sociales y culturales incorporándolas para dar mayor pertinencia a sus aprendizajes.

Todos los funcionarios de la JUNJI, en el desempeño de las labores correspondientes a su cargo, deberán dar cumplimiento a las directrices y lineamientos reflejados en las políticas, normas, planes y procedimientos en materia de seguridad de la información, propendiendo a la mejora continua en esta materia.

Considerando la diversidad de información crítica en JUNJI, como los datos de los funcionarios, sus remuneraciones, datos de Jardines Infantiles de Administración Directa y operados vía Transferencias de Fondos, datos del presupuesto institucional, datos reservados y protegidos como la información del párvulo y sus familias, es necesario asegurar la disponibilidad, integridad y confidencialidad de los activos de información institucional.

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

La información es un activo esencial para la institución y necesita ser administrado y protegido adecuadamente para asegurar la continuidad del servicio. En estos activos de información se distinguen tres niveles básicos:

- La información como tal, ya sea en papel, digital, electromagnética, y otros.
- Los equipos, sistemas e infraestructura que transportan, almacenan, reproducen, eliminan, modifican y/o procesan esta información.
- Las personas que guardan, emiten, transportan y utilizan esta información.

2. POLITICA Y OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

La Junta Nacional de Jardines Infantiles se compromete a gestionar la Seguridad de la Información para asegurar la integridad, confidencialidad y disponibilidad de sus activos de información Institucional con el propósito de dar continuidad operacional en la entrega oportuna, integral y de calidad de educación parvularia para los niños y niñas que asisten a los distintos programas educativos que ofrece la institución a lo largo del país, mediante la identificación, evaluación, priorización y gestión de los controles requeridos a los procesos o servicios que provee, permitiendo con ello, mitigar los riesgos que surgen de fuentes internas o externas a la Institución.

Lo anterior, hace necesario relevar las intenciones de nuestra Institúción en lo relativo a los ejes estratégicos mediante la implementación de una **Política de Seguridad de la Información.**

DE ACUERDO A LO ANTERIOR, NOS COMPROMETEMOS A:
1. Proteger integridad, disponibilidad y confidencialidad de los activos de la información del Servicio contra amenazas que atentan contra el valor, la imagen y la continuidad institucional. 2. Promover una cultura institucional para avanzar en la concientización de todas/os los funcionarios en materias de Seguridad de la información. 3. Gestionar la continuidad de los servicios de tecnologías de información y comunicación. 4. Establecer los mecanismos necesarios para la implementación y mantención de la gestión de seguridad de la información. 5. Cumplir con las normativas legales, regulatorias, contractuales y técnicas vigentes, aplicables en materias de seguridad de la información. 6. Resguardar la información Institucional y sus activos de la información mediante la implementación de controles de acceso.

COMPROMISOS	OBJETIVOS
1. Proteger integridad, disponibilidad y confidencialidad de los activos de la información del Servicio contra amenazas que atentan contra el valor, la imagen y la continuidad institucional.	a. Inventariar los activos de información relevantes para la institución. b. Identificar las vulnerabilidades y amenazas asociadas a los activos de información inventariados. c. Gestionar el tratamiento de las vulnerabilidades identificadas.
2. Promover una cultura institucional para avanzar en la concientización de todas/os los funcionarios en materias de Seguridad de la información.	a. Establecer un plan de difusión institucional para relevar la importancia de la seguridad de la información.
3. Gestionar la continuidad de los servicios de tecnologías de información y comunicación.	a. 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.
4. Establecer los mecanismos necesarios para la implementación y mantención de la gestión de seguridad de la información.	a. Diseñar, implementar y mantener un procedimiento para la gestión de Seguridad de la Información.
5. Cumplir con las normativas legales, regulatorias, contractuales y técnicas vigentes, aplicables en materias de seguridad de la información.	a. Resguardar que los procedimientos estén en conformidad con la normativa legal vigente en materia de seguridad de la información.
6. Resguardar la información Institucional y sus activos de la información mediante la implementación de controles de acceso.	a. Revisar y actualizar la política de control de acceso de seguridad de la información. b. Definir una estrategia institucional para promover buenas prácticas en materia de Control de Acceso a la información. c. Resguardar la información institucional en la gestión de servicios prestados por terceros.

JUNTA NACIONAL DE JARDINES INFANTILES
FISCALÍA

3. ÁMBITO DE APLICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

La presente política es aplicable a la gestión de funcionarios de planta, contrata y al personal que se desempeñe en la calidad a honorarios que formen parte de la JUNJI, y en general a cualquier otra persona o empresa que preste servicios o se encuentre contratado por la Institución, mediante un proceso gradual que se implementará en la Dirección Nacional, posteriormente en las Direcciones Regionales, para finalizar en los establecimientos y Programas Educativos con que cuenta la institución.

Para gestionar la Seguridad de la Información, se consideran como referentes los requisitos de la norma NCh-ISO 27001.Of2013 y las orientaciones de implementación indicadas en la NCh-ISO 27002.Of2013.

El alcance de la gestión de seguridad de la información es determinado y documentado en un proceso de definición que debe orientarse hacia los productos estratégicos de la institución.

4. ROLES Y RESPONSABILIDADES.

La Vicepresidenta Ejecutiva designa a los miembros del Comité de Seguridad de la Información, al Encargado Nacional y Encargados/as Regionales de Seguridad de la Información mediante resolución exenta.

El rol del Comité es gestionar las políticas de seguridad de la información, reuniendo la representación y presencia de los distintos departamentos y unidades de la JUNJI. Sus tareas específicas son:

a. Aprobar e implementar las políticas de seguridad de la información y de control de acceso, proponiendo estrategias y soluciones específicas para el establecimiento de los controles preventivos y/o correctivos asociadas a situaciones de riesgo de seguridad de la información.
b. Evaluar la eficacia de la implementación de procedimientos específicos y estándares que se desprenden de las políticas de seguridad de la información y de control de acceso.
c. Arbitrar conflictos en materia de seguridad de la información.
d. Coordinar su gestión con los Comités de Calidad y de Riesgos, para mantener alineadas las estrategias comunes de gestión Institucional.
e. Reportar, en conjunto con el Encargado de Seguridad de la Información, a la Vicepresidencia Ejecutiva, respecto de oportunidades de mejora en la Gestión de la Seguridad de la Información, así como de los incidentes relevantes y su posible solución.

El rol del Encargado Nacional de Seguridad de la Información es:

a. El desarrollo inicial de las políticas de seguridad de la información al interior de la institución, el control de su implementación y asegurar su aplicación.
b. Coordinar las gestiones para el tratamiento de incidentes que afecten a los activos de información institucional.
c. Establecer puntos de enlaces con Encargados de Seguridad de la Información de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.
d. Las demás tareas que se le asignen por la Vicepresidenta Ejecutiva de JUNJI en cumplimiento de la política institucional en materia de seguridad de la información.

El rol de los Encargados Regionales de Seguridad de Información es:

a. Velar por la estricta aplicación de controles de seguridad de la información que emanen de los lineamientos definidos por el Comité de Seguridad de la Información.

JUNTA NACIONAL DE JARDINES INFANTILES
FISCALÍA

5. POLÍTICA, OBJETIVOS Y PROCEDIMIENTO DE CONTROL DE ACCESO.

La Junta Nacional de Jardines Infantiles, de acuerdo a los compromisos establecidos en la Política de Seguridad de la Información, en lo referido a resguardar la información Institucional y sus activos de la información, asume la implementación de una ***Política de Control de Acceso*** con los siguientes objetivos:

Objetivos	Actividades
1. Revisar y actualizar la política de control de acceso de seguridad de la información.	a. Revisar y actualizar la política de control de acceso de seguridad de la información.
2. Definir una estrategia institucional para promover buenas prácticas en materia de Control de Acceso a la información.	a. Identificar las Áreas Seguras y sus requerimientos. b. Identificar y establecer los requisitos de acceso físico a las instalaciones de la Institución. c. Identificar los requerimientos de seguridad de cada una de las aplicaciones. d. Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de estaciones de trabajo y las redes de datos de la institución. e. Asegurar el cumplimiento de los requisitos normativos, estatutarios, reglamentarios y contractuales, que estén orientados hacia el control de acceso en la JUNJI.
3. Resguardar la información institucional en la prestación de servicios de terceros.	a. Asegurar la protección de los activos de información de la JUNJI a los que tienen acceso sus proveedores. b. Se deben abordar y documentar junto con el proveedor los requisitos de seguridad de la información.

5.1 Alcance de la Política de Control de Acceso

Esta política se aplica a todos los funcionarios, servidores públicos a honorarios y terceros que tengan derechos de acceso a la información, que puedan afectar los activos de información de la Junta Nacional de Jardines Infantiles y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

5.2 Marco Referencial

El marco referencial de la Política de Control de Acceso de JUNJI consta de sus declaraciones de propósitos institucionales y todo lineamiento en apoyo de los objetivos y principios de la seguridad de la información.

Los contenidos y controles esenciales de carácter legal que debe considerarse en las políticas de JUNJI son:

- NCh-ISO 27002.Of2013- Tecnologías de la Información y Código de prácticas para los controles de seguridad de la información - INN Chile.
- Ley 20.285 regula el principio de transparencia de la función pública y el derecho de acceso a la información de los órganos de la Administración del Estado.
- Ley 19.628 de Protección de vida privada y datos.
- Ley 19.223 de Delitos informáticos.

JUNTA NACIONAL DE JARDINES INFANTILES
FISCALÍA

- Decreto Supremo Nº83 – Norma Técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.
- Ley 17.336 de 1970, Sobre Propiedad Intelectual.

5.3 Control de Accesos.

a) Reglas para el control de acceso.
Las reglas para el control de acceso a los recursos tecnológicos, estará documentado a través de diferentes procedimientos.

b) Control de acceso físico.
La institución debe implementar los procedimientos y disponer de los recursos para cumplir con los siguientes controles de acceso físico:

- El personal de JUNJI y el personal de terceros autorizados, deben portar siempre su identificación en un lugar visible al permanecer en las áreas seguras.
- Las visitas autorizadas que fueran a ingresar a áreas seguras se les debe exigir su identificación y firma en el registro de ingreso. Se les debe entregar una tarjeta de visita, la que se debe portar en lugar visible. Las visitas no pueden trasladarse entre áreas seguras sin el acompañamiento de un funcionario JUNJI.
- El acceso a las áreas seguras debe estar físicamente restringido. El tipo y fortaleza de esta restricción física debe estar acorde a la criticidad de los activos de información en el área segura.

c) Gestión de credenciales de acceso lógicas:
Se deberá asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información. La asignación de nuevas credenciales de accesos a los diferentes sistemas se debe solicitar al Área de Atención de Usuarios de la Unidad TI, generándose registro con el nombre del sistema, nombre usuario, contraseña temporal y la asignación de derechos al sistema y/o los servicios. Para usuarios existentes, la creación, modificación y eliminación de permisos y credenciales se deben solicitar al Área de Atención de Usuarios de la Unidad TI.

d) Responsabilidad de los usuarios:
Todos los funcionarios o terceros que tengan un usuario de la red institucional, deberán conocer y cumplir con el uso de esta Política específica, donde se dictan pautas sobre derechos y deberes con respecto al uso adecuado de los activos de información, así como políticas de protección de equipo de usuario desatendido, escritorio y pantalla limpia.

e) Control de acceso a la red:
Las conexiones no seguras a los servicios de red pueden afectar a toda la institución, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.
Las reglas de acceso a la red a través de los puertos, estarán basadas en la premisa *"todo está restringido, a menos que este expresamente permitido"*.

f) Política de utilización de los servicios de red:
Se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

- Controlar el acceso a los servicios de red tanto internos como externos.
- Identificar las redes y servicios de red a los cuales se permite el acceso.
- Dictar normas y elaborar procedimientos de autorización de acceso entre redes.
- Establecer controles y procedimientos de administración para proteger el acceso y servicios de red.

g) Autenticación de usuario para conexiones externas:

La Unidad de Tecnologías de la Información (TI) contempla servicios de conexiones externas para funcionarios o terceros que requieran conexión remota a la red de datos institucional. El acceso a estos servicios es restringido y protegidos mediante credenciales de acceso.

h) Identificación de equipos en la red:
La Unidad de Tecnologías de la Información (TI) controlará e identificará los equipos conectados a su red, mediante el uso de controladores de dominio, asignación manual de IP y conexión WIFI.

i) Protección de los puertos de configuración y diagnóstico remoto:
Los puertos que permitan realizar mantenimiento y soporte remoto a los equipos de red, servidores y equipos de usuario final, estarán restringidos a los administradores de red o servidores.
Los usuarios finales deberán permitir tomar el control remoto de sus equipos para el Área de Soporte, teniendo en cuenta, no tener archivos con información sensible a la vista, y no desatender el equipo mientras se tenga el control del equipo por un tercero.

j) Control de conexión de las redes:
Dentro de la red de datos institucional se restringirá el acceso a:

- La telefonía a través de internet.
- Correo electrónico comercial no autorizado.
- Descarga de archivos de sitio peer to peer.
- Conexiones a sitios de streaming no autorizado.
- Acceso a sitios de pornografía.
- Cualquier otro servicio que vulnere la seguridad de la red o degrade el desempeño de la misma.

k) Control de enrutamiento de red:
El acceso a redes desde y hacia afuera de la Institución cumplirá con los lineamientos de Control de acceso a la red y adicionalmente se utilizaran métodos de autenticación de protocolo de enrutamiento, rutas estáticas, traducción de direcciones y listas de control de acceso.

l) Acceso a internet:
La Unidad de Tecnología de la Información, proveerá a través de sus ISPs (Proveedor de Servicio de Internet) el servicio de internet institucional, el cual será administrado por el proceso de direccionamiento tecnológico y será el único servicio de internet autorizado.

5.4 Control de acceso al sistema operativo:

a) Registro de inicio seguro:
El acceso a los sistemas operativos estará protegido, mediante un inicio seguro de sesión, que contemplará las siguientes condiciones:

- No mostrar información del sistema, hasta que el proceso de inicio se haya completado.
- No suministrar mensajes de ayuda, durante el proceso de autenticación.
- Validar los datos de acceso, una vez que se han diligenciado todos los datos de entrada.
- Limitar el número de intentos fallidos de conexión auditando los intentos no exitosos.
- No mostrar las contraseñas digitadas.
- No transmitir la contraseña en texto claro.

b) Gestión de contraseñas.
La asignación de contraseñas se deberá controlar a través de un proceso formal y cumplir con los requisitos dispuestos por el Área de Atención de Usuarios de la Unidad TI. Las recomendaciones son:

- No escribirlas en papeles de fácil acceso, ni en archivos sin cifrar.
- No habilitar la opción — recordar clave en este equipo, que ofrecen los programas.
- No enviarla por correo electrónico.
- Nunca guarde sus contraseñas, en ningún tipo de papel, agenda, etc.
- Las contraseñas se deben mantener confidenciales en todo momento.
- No compartir las contraseñas, con otros usuarios.
- Cambiar la contraseña si existe sospecha de que alguien más la conoce y si ha tratado de dar mal uso de ella.
- Seleccionar contraseñas que no sean fáciles de adivinar.
- Nunca grabar la contraseña en una tecla de función o en un comando de caracteres predefinido.
- Cambiar las contraseñas regularmente.
- No utilizar la opción de almacenar contraseñas en Internet.
- No utilizar contraseña con números telefónicos, nombre de familia etc.
- No utilizar contraseña con variables (soporte1, soporte2, soporte3 etc.).

c) Uso de utilitarios del sistema.
El uso de utilitarios licenciados del sistema, estará restringido a usuarios administradores. Se establecerá una política a nivel del controlador de dominio, que no permita la instalación de software y cambios de configuración del sistema. Ningún usuario final deberá tener privilegios de usuario administrador.

d) Tiempo de inactividad de la sesión.
Después de cinco (5) minutos de inactividad del sistema, se considerará tiempo muerto y se bloqueará la sesión, sin cerrar las sesiones de aplicación o de red. Los usuarios procederán a bloquear sus sesiones cuando deban abandonar temporalmente su puesto de trabajo. Las estaciones de trabajo deberán quedar apagadas al finalizar la jornada laboral o cuando una ausencia temporal supere dos (2) horas.

e) Limitación de tiempo de conexión.
Por la misión de la Unidad de Tecnologías de la Información, no se limitará el tiempo de conexión, ni se establecerán restricciones en la jornada laboral.

f) Control de acceso a la información.
El control de acceso a la información a través de una aplicación, se realizará a través de roles que administren los privilegios de los usuarios dentro del sistema de información.

El control de acceso a información física o digital, se realizará teniendo en cuenta los niveles de clasificación y el manejo de intercambio de información.

g) Aislamiento de sistemas sensibles.
La Unidad de Tecnologías de la Información, identificará según los niveles de clasificación de información cuales sistemas considera sensibles y que deberían gestionarse desde ambientes tecnológicos aislados e independientes.

Al aislar estos sistemas se debe prever el intercambio seguro de información, con otras fuentes de datos, ya que no se permite duplicar información en otros sistemas, siguiendo las directrices de fuentes únicas de datos.

5.5 Acceso desde terminales móviles y trabajo remoto.

Teniendo en cuenta las ventajas de la computación móvil y el trabajo remoto, así mismo el nivel de exposición a amenazas que pongan en riesgo la seguridad de la información institucional, a continuación se establecen directrices que permitirán regular el uso de la computación móvil y trabajo remoto.

a) Computación y comunicaciones móviles.
Se entiende como dispositivos de cómputo y comunicación móviles, todos aquellos que permitan tener acceso y almacenar información institucional, desde lugares diferentes a las instalaciones.

El uso de equipos de cómputo y dispositivos de almacenamiento móviles, está restringido únicamente a los provistos por la institución y deberán contemplar las siguientes directrices:

- Uso de usuario y contraseña para acceso al mismo.
- Cifrado de la información.
- Uso de software antivirus provisto por la Unidad de Tecnologías de la Información.
- Restricción de privilegios administrativos para los usuarios.
- Uso de software licenciado y provisto por la Unidad de Tecnologías de la Información.
- Realización de copias de seguridad periódicas.
- Uso de mecanismos de seguridad que protejan la información en caso de pérdida o hurto de los dispositivos.
- Permanecer siempre cerca del dispositivo.
- No dejar desatendidos los equipos.
- No llamar la atención, acerca de portar equipos móviles.
- No identificar el dispositivo con distintivos de la Unidad de Tecnologías de la Información.
- No colocar datos de contacto técnico en el dispositivo.
- Mantener cifrada la información clasificada.
- No conectarse a redes WiFi públicas.
- Mantener apagado el Bluetooth o cualquier otra tecnología inalámbrica.
- Informar de inmediato al Área de Atención de Usuarios de la Unidad TI sobre la pérdida o hurto del dispositivo, quien procederá al bloqueo del usuario.

Para dispositivos de comunicación móvil (telefonía celular) institucionales se aplicaran los controles antes mencionados y los detallados a continuación:

- Activar la clave del teléfono, para acceso a la agenda telefónica, mensajes de texto, llamadas entrantes, salientes, perdidas. Archivos de voz, imagen y videos.
- No hablar de temas confidenciales cerca de personas que no requieran conocer dicha información.

b) Trabajo Remoto.
El trabajo remoto solo será autorizado por el responsable de la unidad organizativa de la cual dependa el funcionario que solicite el permiso.

6. GESTIÓN DE DOCUMENTACIÓN DE SEGURIDAD DE LA INFORMACIÓN

6.1 Aprobación de Políticas y otros Documentos.

Las políticas específicas de seguridad de la información y otros documentos, serán generadas y aprobadas según las normas generales de la administración pública, atendiendo a los lineamientos y prácticas de seguridad particular o transversal, conforme a su estructura y requerimientos de seguridad.

6.2 Control de Documentos.

Los documentos requeridos para gestionar la seguridad de la información, deben protegerse y controlarse. Para lograr este objetivo, las acciones necesarias a implementar son:

- Revisar y actualizar los documentos cuando sea necesario y aprobarlos nuevamente.
- Registrar todos los cambios o actualizaciones a los documentos en la tabla de control de cambios.
- Los registros de las actualizaciones o modificaciones en la tabla de control de cambio deben ser coincidentes con el texto del respectivo documento.
- Los registros de las tablas de cambio deben ser legibles y fácilmente identificables en el documento respectivo.
- Se deberá controlar el uso no intencionado de documentos obsoletos.
- En caso de mantenerse los documentos por cualquier propósito, éstos deberán tener una adecuada identificación a efecto de diferenciarse de los vigentes.
- Las versiones pertinentes de los documentos aplicables se encontrarán disponibles para quienes lo necesiten y serán almacenados y transferidos de acuerdo a los procedimientos aplicables a su clasificación.

6.3 Publicación y Comunicación de Políticas y otros Documentos

Las versiones vigentes de políticas y documentos vinculadas a la Gestión de Seguridad de la Información serán publicadas a través de los canales de información institucionales.

La difusión de las políticas específicas de seguridad de la información, los procedimientos y otros documentos se efectuará de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, pudiendo utilizarse los canales de información institucionales.

6.4 Revisión de Políticas y otros Documentos

Las políticas específicas de seguridad de la información y otros documentos, serán revisados cada dos años, o cuando JUNJI lo requiera, para asegurar su continuidad e idoneidad, considerando los cambios que puedan producirse, tales como: enfoques a la gestión de seguridad de la información, circunstancias de la Institución, cambios legales, cambios tecnológicos, instrucciones que emanen de autoridades pertinentes, recomendaciones frente a amenazas y vulnerabilidades, entre otras.

7. SANCIONES APLICABLES

El incumplimiento o violación de una política específica de seguridad de la información, debidamente acreditado, conlleva a través de un procedimiento disciplinario, a la aplicación de medidas disciplinarias previstas en el Estatuto Administrativo, respecto a los funcionarios de JUNJI, o al término anticipado del contrato por incumplimiento de obligaciones, cuando se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de la presente política, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

8. GLOSARIO

Proceso:
Conjunto de actividades relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.

Política:
Conjunto de principios o reglas declaradas por la institución, a través de su Vicepresidencia Ejecutiva, para guiar la toma de decisiones y obtener los productos correctos.

Disponibilidad:
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:
Atributo de la información, que establece que ésta solo esté disponible o se revele a individuos o procesos autorizados.

Integridad:
Atributo de la información, que permite entender que ésta se encuentra completa, actualizada y es verás, sin modificaciones inapropiadas o corruptas.

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

Comité de Seguridad de la Información:
Entidad funcional responsable de implementar las políticas de seguridad de la información.

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

Seguridad de la Información:
Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades, tales como autenticidad, responsabilidad con obligación de informar, no repudio y confiabilidad norma chilena oficial NCh-ISO 27001.Of2013.

Infraestructura:
Base física que soporta sistemas, equipamientos y la información en sí. Incluye edificios, salas, cableados, muebles, contenedores, bodegas y otros.

Área Segura:
Espacios que contienen ya sea información sensible o crítica y las instalaciones de procesamiento de información.

JUNTA NACIONAL DE JARDINES INFANTILES
FISCALÍA

3° DESÍGNASE como Encargado Nacional de Seguridad de la Información para la Junta Nacional de Jardines Infantiles, para los efectos dispuestos en el artículo 12, del Decreto Supremo N°83, del año 2004, del Ministerio Secretaría General de la Presidencia, a don CHRISTIAN CÓRDOVA TORRES, Cédula de Identidad N° 13.431.162-2, Director del Departamento de Planificación de la Institución, o en su defecto a quien lo subrogue en dicho cargo.

4° DESÍGNANSE como Encargados Regionales de Seguridad de la Información de la Junta Nacional de Jardines Infantiles, para los efectos dispuestos en el artículo 12, del Decreto Supremo N°83, del año 2004, del Ministerio Secretaría General de la Presidencia, a los Directores/as Regionales de este Servicio, o aquellos funcionarios que estos designen en su representación, a fin de que velen por la estricta aplicación de controles de seguridad de la información, que emanen de los lineamientos definidos por el Comité de Seguridad de la Información.

5° ESTABLÉCESE que serán funciones del Encargado Nacional de Seguridad de la Información, las contenidas en el capítulo "Roles y Responsabilidades" del Manual de Políticas Específicas de Seguridad de la Información, aprobado mediante el presente acto administrativo.

6° DESÍGNANSE como miembros del Comité de Seguridad de la Información al Encargado Nacional de Seguridad de la Información, quien lo presidirá, y a todos los Directores/as y Jefes/as de Unidades dependientes de la Vicepresidenta Ejecutiva de la Junta Nacional de Jardines Infantiles o aquellos funcionarios que estos designen en su representación. Lo anterior, sin perjuicio de la asistencia a las sesiones de otros funcionarios/as de la institución convocada al efecto, a fin de asesorar al Comité, dejándose constancia de ello mediante un acta de la reunión.-

7° DETERMÍNASE que el contexto y Alcance de aplicación del Sistema de Gestión de Seguridad de la Información, será el subproceso de **Gestión de Datos de Párvulos,** ejecutado geográficamente en las dependencias de la Dirección Nacional de la Junta Nacional de Jardines Infantiles.

8° DIFÚNDASE el presente Manual de Políticas Específicas de Seguridad de la Información, a todas y todos los funcionarios del Servicio, por la Unidad de Comunicaciones del Servicio, a través del medio que dicha Unidad defina.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

JUNTA NACIONAL DE JARDINES INFANTILES
VICEPRESIDENTA EJECUTIVA

DESIREE LÓPEZ DE MATURANA L.
VICEPRESIDENTA EJECUTIVA
JUNTA NACIONAL DE JARDINES INFANTILES

DLdML/LRM/CCT/SMV/PSV
Distribución:
- Vicepresidencia Ejecutiva
- Directores de Departamento
- Jefes de Unidades de Vicepresidencia Ejecutiva
- Direcciones Regionales
- Oficina de Partes
- Ingreso Depto. de Fiscalía y Asesoría Jurídica (1209 / 2017)

JUNTA NACIONAL DE JARDINES INFANTILES
JUNJI Ministerio de Educación
DEPARTAMENTO DE FISCALÍA