RESOLUCIÓN EXENTA Nº 015/ 00264

REF.: APRUEBA PROCEDIMIENTO PARA LA CONVERSION Y/O TRASPASO DE DATOS; PLAN DE CONTINUIDAD OPERACIONAL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN Y PLAN DE PRUEBAS

SANTIAGO, 23 ABR 2014

VISTOS

1°) La Ley Nº 17.301, que crea la Junta Nacional de Jardines Infantiles; 2°) la Ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, cuyo texto refundido, coordinado y sistematizado fuere fijado mediante D.F.L. Nº 1/19.653, del año 2000, del Ministerio Secretaría General de la Presidencia; 3°) la Ley Nº 19.880, que establece las Bases de los Procedimientos Administrativos que rigen los actos de los Órganos del Estado; 4°) los Decretos Supremos Nº 1.574, del año 1971, y 156, del año 2014, ambos del Ministerio de Educación; 5°) el Decreto Supremo Nº 83, del año 2004, del Ministerio Secretaría General de la Presidencia, que aprueba la norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos; 6°) la Resolución Nº 1.600, del año 2008, de la Contraloría General de la República; 7°) la Resolución Exenta Nº 015/2177, de 28 de diciembre de 2012, de la Vicepresidenta Ejecutiva de la Junta Nacional de Jardines Infantiles, que actualiza política de seguridad de la información para la Junta Nacional de Jardines Infantiles, y demás antecedentes tenidos a la vista.

CONSIDERANDO

1º Que, mediante Decreto Supremo Nº 83, del año 2004, del Ministerio Secretaría General de la Presidencia, se aprobó la norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos, el cual en su artículo 36, mandata a todos los órganos de la Administración del Estado a desarrollar las políticas, procedimientos, acciones y medidas tendientes a la obtención del nivel avanzado de seguridad de los documentos electrónicos.

2º Que, en virtud de dicho mandato, y conforme con lo dispuesto en el artículo 37, del Decreto antes citado, en relación con la Norma Chilena ISO 27.001 y 27.002, se creó y aprobó por la Jefatura Superior del Servicio, la Política General de Seguridad de la Información.

3º Que, en el marco del Sistema de Seguridad de la Información y de acuerdo a lo señalado en la Política General de Seguridad de la Información de la Junta Nacional de Jardines Infantiles, aprobada por Resolución Exenta Nº 015/2177, de 28 de diciembre de 2012, de la Vicepresidenta Ejecutiva uno de los objetivos de la gestión de seguridad de la información es: "*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*".

4º Que, en razón de lo anterior y, en virtud de los hallazgos y compromisos asociados al seguimiento de Auditoría Interna al Departamento de Informática denominada "Auditoría de Evaluación Integral del Sistema de Control Interno Institucional", es necesario dictar el siguiente acto administrativo.

FISCAL

RESUELVO

1º APRUÉBASE el "Procedimiento para la Conversión y/o Traspaso de Datos" del Subdepartamento de Informática, que es del siguiente tenor:

Procedimiento para la Conversión y/o Traspaso de Datos[1]

Contenido

1. Introducción

Todos los datos e información que opera y gestiona la Institución para desarrollar sus funciones son almacenados en: Base de Datos[2]; Computador personal[3] de cada usuario y Carpetas electrónicas[4], ubicadas en servidor de archivo, en razón de ello, se generarán procedimientos para que la conversión y/o traspaso de información se realice de manera controlada, entendiendo por tal, aquella que se solicite y se proporcione por vía formal, y de las cuales quede registro.

Base de Datos

Los Sistemas de Información[5] actualmente en producción generan información que es almacenada en la única Base de Datos (Motor de Base de datos Oracle), la que puede ser consultada o extraída por los usuarios con privilegios[6] y acceso a ellos, a través de los

---

[1] Todas las definiciones que en el presente texto se contienen, han sido proporcionadas por el Subdepartamento de Informática.
[2] Base de Datos: "almacén que permite guardar una gran cantidad de datos de forma organizada y relacionados entre sí, los cuales son recolectados y explotados por los Sistemas de Información."
[3] Computador personal: "aquel computador pequeño, para un solo usuario, que consta de un teclado para introducir datos, un monitor para visualizar la información y un dispositivo de almacenamiento para guardar datos."
[4] Carpetas electrónicas: "repositorio donde se puede almacenar cualquier tipo de archivo y/o documentos electrónicos."
[5] Sistemas de Información: "conjunto de componentes (personas, datos, redes, software y hardware) relacionados entre sí, que recolectan, procesan, almacenan y distribuyen información para apoyar la toma de decisiones y control en la organización".
[6] Usuarios con privilegios: "toda aquella persona (sea funcionario institucional o externo) que tenga el permiso para acceder a dichos datos".

menús respectivos de cada sistema. Sin embargo, hay ciertos requerimientos[7] institucionales de datos almacenados en la Base de Datos, que no pueden ser resueltos a través de un sistema de Información. Para ello, se implementará un procedimiento de manera de traspasar los datos o información requerida, de forma controlada.

Computadores personales

En los computadores personales que utilizan los funcionarios del Servicio para el desarrollo de sus funciones y el cumplimiento del quehacer Institucional, se generan datos e información que en caso de cambio de tecnología o falla del equipo, deben ser traspasados a un nuevo equipo. Para este caso, se generará un procedimiento que permita el traspaso de datos e información controlado.

Carpetas electrónicas compartidas[8]

Existe un servidor de archivo que permite crear Carpetas, conforme a distintos criterios, como por ejemplo: departamentos, materia, etc., con el propósito que los funcionarios institucionales almacenen archivos que pueden compartir entre ellos, sin embargo, por cambio tecnológico o límite de almacenamiento, puede ser necesario traspasar esta información a un nuevo equipo. Para estos casos, se generará un procedimiento que permita el traspaso de información controlado.

2. Objetivo

Disponer de procedimientos para que el traspaso de información, hacia la unidad requirente, se realice de manera controlada. Lo anterior significa, que el Departamento de Informática, que es la unidad que recibe la solicitud y encargada de efectuar el traspaso y/o conversión de datos, cuente con registros de la fecha y solicitud recibida, así como de la unidad requirente, y también de la fecha de traspaso y contenido del mismo.

3. Alcance

Este procedimiento es aplicable en el Servicio para los datos o información de la Base de Datos que no pueden ser extraídos a través de los Sistemas de Información, datos o información de los computadores personales que han sufrido fallas o cambio de equipos y para los datos o información de las carpetas electrónicas compartidas.

---

[7] Requerimientos: "datos solicitados que no están resueltos a través de las consultas establecidas, pero cuya información está almacenada en la base de datos, en forma no estructurada."

[8] Carpetas electrónicas compartidas: "repositorio donde se puede almacenar cualquier tipo de archivo y/o documento electrónico al cual pueden acceder todos los usuarios que cuenten con permiso para ello".

4. Responsabilidad

La responsabilidad de estos procedimientos será del Subdepartamento de Informática.

5. Actualizaciones

El procedimiento se actualizará anualmente, en base a la experiencia observada de los acontecimientos, y se elaborará la mejora respectiva por escrito, a través de un documento.

El registro relativo a las estadísticas referentes a la cantidad de carpetas electrónicas compartidas, computadores personales cambiados, u otras, se incorporarán en la actualización anual.

Historial de Revisiones

Fecha	Versión	Descripción	Autor
06-2013	0.1	Versión Inicial	Claudia Pizarro, Juan Parra, Alvaro Abarza

6. Procedimientos

6.1 Datos e Información de Base de Datos no accesibles por los Sistemas de Información.

- La solicitud de Información o datos no disponible a través de un sistema deberá ser solicitada por el Director requirente respectivo al Director de Departamento dueño de los datos u información, por escrito.
- Si el Departamento requerido no puede dar respuesta a esa solicitud, ésta será enviada al Departamento de Informática.
- El Departamento de Informática analizará la solicitud respectiva, si estima que necesita un mayor análisis para dar respuesta solicitará reunión de trabajo para clarificar requerimientos, generando acta de reunión.

- Una vez aclarados los requerimientos, el Departamento de Informática procederá a generar la respuesta respectiva, la cual enviará al Departamento solicitante a través de Memorándum.
- El Departamento de Informática conservará copia de dicho documento de respuesta.

6.2 Datos y/o Información de computador personal con fallas o cambio de computador personal

- El funcionario requirente deberá informar por Memorándum o por vía escrita alternativa, tal como correo electrónico, al Departamento de Informática, el nombre de las carpetas que existen en el computador personal y el nombre de los archivos que no se encuentran en carpeta que se deben traspasar.
- La Información a traspasar solamente será la Institucional.
- Un funcionario de Informática del área de Soporte realizará el respaldo y solicitará al funcionario requirente el Visto Bueno de la información a traspasar, de modo de asegurarse que no falte nada.
- El funcionario de Informática realizará el traspaso de la Información al nuevo computador personal asignado y solicitará el Visto Bueno al funcionario requirente, a través de un correo electrónico.
- Solamente con el Visto Bueno del funcionario requirente, informática procederá a eliminar la información respaldada.

6.3 Carpetas Electrónicas Compartidas

- Un funcionario de Informática informará al Jefe del Departamento dueño de la información almacenada en la carpeta, sobre la solicitud de traspaso de información.
- Con la autorización del Jefe del Departamento respectivo, el funcionario de informática procederá a efectuar un respaldo de la carpeta solicitada, luego de lo cual, procederá al traspaso de la información solicitada.
- Una vez traspasada la información se solicitará revisar que su contenido corresponda con lo solicitado, para luego, aprobar el traspaso.
- Solamente con dicha aprobación, se procederá a operar con la nueva carpeta y eliminar la carpeta antigua.

- Respecto de la carpeta de respaldo, si el funcionario lo solicita, informática hará entrega de un DVD que contenga la información respaldada. Si no lo hace, ésta será eliminada, una vez que se haya aprobado el traspaso.

2º APRUÉBASE el "Plan de Continuidad Operacional de las TIC" del Departamento de Informática, que es del siguiente tenor:

Plan de Continuidad Operacional de las Tecnologías de la Información y Comunicación

Contenido

1. Introducción

Con el propósito de mantener una alta probabilidad de continuidad operacional de los procesos de provisión de productos estratégicos, procesos de soporte y canales de comunicación ante posibles desastres o incidentes de fuerza mayor, como cortes de energía eléctrica por periodos prolongados, inundaciones, terremotos, fallas en los equipos o desastres de la naturaleza, se hace imprescindible contar con planes de continuidad para la plataforma tecnológica actualmente disponible en la JUNJI, de modo, que sea posible actuar ante estas contingencias potenciales.

No contar con información de los sistemas de Información, información almacenada en la Base de Datos institucional e información de Correos Electrónicos por caídas de la plataforma tecnológica, puede originar falta de información para la toma de decisiones, desactualización de antecedentes, atención ineficiente e incumplimiento de compromisos o un sinnúmero de otros efectos negativos que pueden ser muy significativos para la Institución. Razón por la cual, el Plan de Continuidad se centrará en la "plataforma tecnológica crítica", que en definitiva permitirá la continuidad del quehacer Institucional.

Se entiende por "Plataforma Tecnológica Crítica" el conjunto de Hardware[9] y Software[10] que ante cualquier falla, pone en riesgo la continuidad operacional de la Institución.

Por lo tanto, los procedimientos para la continuidad de la operación que apoyan el proceso de recuperación de la plataforma tecnológica posterior a cualquier evento que los afecte parcial o totalmente serán para enlace[11] de comunicaciones y energía eléctrica, servidores y sistemas de información, que a continuación se detallan:

Enlace de Comunicaciones y Energía Eléctrica:

- Enlace de Telecomunicaciones
- Servicio de Energía Eléctrica
- Aire Acondicionado en Sala de Servidores

Servidores:

- Servidor de Base de Datos
- Servidor de Aplicaciones
- Servidor de Correo
- Servidor Web

Sistemas de Información:

- Sistemas de Información de la Institución

2. Objetivo

Minimizar el impacto que las incidencias, como desastres naturales, corte de energía y falla física en equipos, podrían producir en la operación normal de la plataforma tecnológica institucional.

3. Alcance

[9] Hardware, está integrado por: Servidor de Base de datos; servidor de aplicaciones; servidor de correo electrónico; servidor web.
[10] Software, está integrado por: Sistema operativo; base de datos; servidor de aplicaciones; correo electrónico; sistemas de información.
[11] Enlace: "medio de conexión entre dos lugares físicos con el propósito de enviar y recibir datos y/o información".

Este plan aplica a la plataforma tecnológica institucional para enfrentar situaciones de desastre que afecten el área de tecnología, en comunicaciones, servidores y sistemas de información.

4. Responsabilidad

La responsabilidad del plan de continuidad de las tecnologías de la información y de la comunicación, es del Subdepartamento de Informática.

5. Actualizaciones

Cada año se revisará para actualizarlo.

Historial de Revisiones

Fecha	Versión	Descripción	Autor
06-2013	0.1	Versión Inicial	Alvaro Abarza

6. Descripción del Plan

Plataforma Tecnológica Crítica	Riesgo	Procedimiento
Enlace de Telecomunicación	Al fallar este servicio la institución no puede operar la plataforma tecnológica para desarrollar sus funciones normalmente.	Servicio con contrato de arriendo a proveedor externo, con dos enlaces, uno primario para operación y otro secundario para respaldo. En caso de falla: • Funcionario de Informática llama e informa a proveedor, por alguna vía de comunicación distinta a la contratada, por ejemplo: celular. • Proveedor opera sobre enlace secundario de respaldo. • Proveedor corrige anormalidad del enlace primario, hasta reestablecer

		el servicio por este enlace e informa a Informática.
Energía Eléctrica en Sala de los Servidores	Al fallar este servicio, los usuarios institucionales no podrán utilizar servicios de correo electrónico, sistemas de información, servicios Web ni autentificación[12] hasta que se resuelva la falla eléctrica que afecte a estos servidores.	Se dispone de un circuito independiente en sala de servidores En caso de fallas • Funcionario de informática informa a Subdepartamento de Cobertura e Infraestructura, responsable por este servicio. • Unidad Organizacional Responsable corrige. • Informática levanta los servicios y los deja operativo.
Aire Acondicionado	Al fallar este servicio aumenta la temperatura en la Sala de Servidores, los servidores que operan allí dejan de funcionar, la institución no puede generar las actividades o funciones que realiza sobre la plataforma tecnológica.	Servicio con contrato de mantención correctiva y preventiva, y tiempos comprometidos en caso de falla (con mantenciones programadas) En caso de Falla: • Funcionario de Informática informa a proveedor. • Proveedor corrige falla. • Proveedor deja operativo equipos de aire acondicionado.
Servidor de Base de Datos y Aplicaciones	Al fallar estos (dos) equipos la Institución no puede operar los Sistemas de información, afectando servicios como, el pago de remuneraciones, el ingreso de datos de los párvulos entre otros servicios.	Servicio con contrato de arriendo y tiempo de respuestas comprometidos. En caso de falla: • Funcionario de Informática llama a proveedor informando falla. • Proveedor soluciona problema dentro de los tiempos comprometidos. • Proveedor reestablece servicio.
Servidor de Correo Electrónico	Al fallar este servicio la Institución no puede hacer uso del servicio de mensajería.	Servicio virtualizado en dos máquinas, máquina N°1 donde opera el aplicativo, máquina N°2 un clone de la máquina N°1 (contiene el respaldo de máquina N°1) En caso de falla • Funcionario de informática opera máquina N°2, queda en funcionamiento. • Máquina N°1 entra en mantención y una vez corregida la falla se pone en operación.
Servidor web	Al fallar este servicio	Servicio virtualizado en dos máquinas,

[12] Autentificación: "proceso de confirmación de la identidad del usuario que generó un documento electrónico y/o que utiliza un sistema informático" (Art.5 a) del D.S. N°83, de 2004)

	la comunidad queda sin acceso al servicio publicado en este sitio.	máquina N°1 donde opera el aplicativo, máquina N°2 clone de la máquina N°1 (contiene el respaldo de máquina N°1) En caso de falla • Funcionario de informática opera máquina N°2, queda en funcionamiento. • Máquina N°1 entra en mantención y una vez corregida la falla se pone en operación.
Sistemas de Información	Al fallar los Sistemas de Información la institución no puede generar las actividades o funciones que se desempeñan en los sistemas, como por ejemplo el, pago de remuneraciones, ingreso y salida de datos de párvulos, entre otras funciones.	Se disponen de los programas fuentes En caso de falla • Se corrigen programas fuentes • Se instala versión de programas fuentes corregidas

3º APRUÉBASE el "Plan de Plan de Pruebas" del Subdepartamento de Informática, que es del siguiente tenor:

PLAN DE PRUEBA

Contenido

1. Introducción

Conscientes que situaciones de contingencia extrema puede presentarse en cualquier momento, como por ejemplo, en horario de oficina, que pueda resultar impactante durante las actividades que desarrolla JUNJI y por lo tanto convertirse en un problema prioritario de atender, es que se hace necesario definir todas las acciones necesarias para asegurar que, en caso real de contingencia, disponer de un conjunto de prestaciones y funcionalidades mínimas que permitan posteriormente ejecutar el plan de continuidad operacional de las Tecnologías de la Información y Comunicación (TIC) de manera rápida y segura.

2. Objetivos

- Programar la prueba y validación de todas las actividades que se llevarán a cabo como parte del plan respecto a una posible interrupción de los procesos identificados como críticos (Plan de Continuidad Operacional TIC) para el servicio de la Institución.
- Identificar por medio de la prueba, las posibles causas que puedan atentar contra la normal ejecución y las medidas correctivas a aplicar para subsanar los errores o deficiencias que se deriven de ella (retroalimentación del plan).
- Determinar los roles y funciones que cumplirán los responsables en la prueba, los mismos que serán los asignados para su ejecución en caso de una situación real de contingencia.

3. Alcance

Dado que plan de Continuidad Operacional está orientado a temas de siniestros cuyas situaciones son imposibles de reproducir en la vida real, es que el plan de pruebas estará enfocado principalmente a simular situaciones de contingencia en caso de incidencias producidas sobre equipos y procesos, manejados en situaciones reales y cuyos respaldos si pueden ser empleados y replicados en una hipotética situación de contingencia.

4. Plan de Prueba Enlace de Telecomunicaciones

4.1. Objetivo

- Probar Enlace de comunicaciones de respaldo

4.2. Alcance

- Área: Departamento de Informática
- Rol : Encargado de Comunicaciones y Seguridad de la Información

4.3. Descripción de la Prueba

Encargado de Comunicaciones deberá coordinar con empresa Entel:

- Fecha y horario de realización de la prueba.
- Entel realizará bajada de Enlace Primario y Subida de Enlace de respaldo.
- Entel realizará subida de Enlace primario.
- Encargado de Comunicaciones registrará prueba en Registro Plan de Prueba.

4.4. Frecuencia

- Una vez en el año

5. Plan de Prueba Aire Acondicionado

5.1. Objetivo

- Probar funcionamiento de Aire Acondicionado

5.2. Alcance

- Área: Subdepartamento de Informática
- Rol: Encargado de Comunicaciones y Seguridad de la Información

5.3. Descripción de la Prueba

Encargado de Comunicaciones y Seguridad de la Información deberá:

- Coordinar con empresa que presta el servicio de mantención fecha y horario de realización de la prueba.
- Dar a conocer a usuarios institucionales tiempo que tomara la realización de las pruebas.
- Bajar máquinas de Aire Acondicionado.
- Llamar a empresa que presta el servicio de mantención.
- Instruir a empresa la puesta en marcha de las máquinas de aire acondicionado.
- Registrar realización de las pruebas en Registro Plan de Prueba.

5.4. Frecuencia

Una vez en el año.

6. Plan de Prueba Servidor de Base de Datos y Aplicaciones

6.1. Objetivo

Probar puesta en operación Servidor de Base de Datos y Servidor de Aplicación.

6.2. Alcance

Área: Departamento de Informática

Rol: Administrador de Base de datos

6.3. Descripción de la Prueba

Administrador de Base de Datos deberá:

- Coordinar con Empresa que presta el servicio de Administración de Base de Datos fecha y horario para realizar prueba de subida y puesta en operación de los servidores de Base de Datos y Aplicación.
- Dar a conocer a los usuarios institucionales los tiempos que tomará la ejecución de esta prueba.
- Instruir a empresa bajada de los servidores.
- Instruir a empresa subida los servidores.
- Instruir a empresa la puesta en operación normal de los servidores.
- Registrar la realización de la prueba en Registro Plan de Prueba.

6.4. Frecuencia

Dos veces en el año

7. **Plan de Prueba Servidor de Correo Electrónico y Servidor Web**

En relación a estos equipos, no se realizará plan de pruebas dado que en el corto plazo serán trasladados a un data center externo y en la actualidad estas máquinas se encuentran virtualizadas lo que implica una probabilidad de 99% de disponibilidad operativa.

ANEXO 1: Registro Plan de Prueba

Registro Plan de Prueba

Control y certificación de pruebas de contingencia

Procesos y/o equipos en prueba: _____

_____

Departamento Responsable: _____

Área Responsable: _____

Fecha____/____/____ Horario Inicio: ____:_____ Horario Final: _____:_____

Alcance: _____

_____

Resultado: Satisfactorio ☐ Satisfactorio con observaciones ☐ Deficientes ☐

Observaciones: _____

_____

_____

_____

_____

Sugerencias para actualizar Plan de Continuidad:

_____

_____

_____

_____

_____

Participantes V°B° y Aprobación

Participantes	Cargo	Firma

4º DIFÚNDANSE las presentes directrices, a todas y todos los funcionarios del Servicio, conforme con los lineamientos correspondientes emanados del Encargado de Seguridad de la Información.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

JUNTA NACIONAL DE JARDINES INFANTILES
VICEPRESIDENTA EJECUTIVA

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

JUNTA NACIONAL DE JARDINES INFANTILES
DE FISCALÍA

DLdeM/LHM/MJS/MCM/JPE/MLD/ mld
Distribución
- Vicepresidenta Ejecutiva
- Directores/Directoras Departamentos y Subdepartamentos
- Directores/Directoras Regionales
- Encargado de Seguridad de la Información (F. Rodríguez)
- Oficina de partes