GOBIERNO DE CHILE
JUNTA NACIONAL DE AUXILIO
ESCOLAR Y BECAS

APRUEBA POLÍTICA Y PROCEDIMIENTO DE RESPALDO DE INFORMACIÓN QUE INDICA, EN EL MARCO DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN DE LA JUNTA NACIONAL DE AUXILIO ESCOLAR Y BECAS.

RESOLUCIÓN EXENTA N° 3163

SANTIAGO, 30-11-2017

VISTO:

Lo dispuesto en la Ley N° 15.720 que crea la Junta Nacional de Auxilio Escolar y Becas; en la Ley N° 19.880, que establece Bases de los Procedimientos Administrativos que rigen las Actas de los Órganos de la Administración del Estado; en el Decreto Supremo del Ministerio de Educación N° 5.311 de 1968, que aprueba el Reglamento General de JUNAEB; en el Decreto Ley del Ministerio de Educación N° 180 de 1973, que declara receso del consejo de JNAEB cuyas facultades otorga a su Secretario General; en el Decreto Supremo del Ministerio Secretaría General de Gobierno N°83 del 2005, que aprueba Norma Técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos; Decreto Supremo del ministerio de Secretaría General de Gobierno N° 77 del 2004, que aprueba Norma Técnica sobre eficiencia de las comunicaciones electrónicas entre órganos de la Administración del Estado y entre estos los ciudadanos del Ministerio Secretaría General de la Presidencia; en el Decreto exento del Ministerio de Educación N° 1106 de noviembre de 2016 que nombra a don Jaime Tohá Lavanderos como Secretario General (S) de la Junta Nacional de Auxilio Escolar y Becas; y 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.

CONSIDERANDO:

1. Que en virtud del Decreto Exento del Ministerio de Hacienda N° 194 de 17 de mayo de 2017, que modifica el Decreto Exento 290 de agosto de 2016, se aprueba el Programa Marco de los Programas de Mejoramiento de la Gestión (PMG) para el año 2017; el cual consta de dos áreas prioritarias y tres sistemas de gestión con sus respectivos objetivos, debiendo los servicios formular compromisos en uno o más sistemas de gestión, dependiendo del grado de desarrollo alcanzado a la fecha de la formulación.

2. Que, en lo que respecta a la Junta Nacional de Auxilio Escolar y Becas, uno de los Programas de Mejoramiento de Gestión dice relación

con el Sistema de Seguridad de la Información, correspondiente al área de Calidad de Servicio y que tiene por objetivo de gestión "*Gestionar los riesgos de seguridad de la información de los activos que soportan los procesos de provisión de bienes y servicios, mediante la aplicación de controles basados en la Norma NCH-ISO 27001 Of2013 del Instituto Nacional de Normalización, sobre Sistemas de Seguridad de la Información*".

3. Que, en este sentido, la referida la Norma NCHI-ISO 27001 Of2013; dispone en el punto 4.4 denominado "*Sistema de Seguridad de la Información" que "la organización debe establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, según los requerimientos de esta norma*"

RESUELVO:

ARTÍCULO 1°: **APRUEBASE** el siguiente documento relativo al Sistema de Seguridad de la Información de la Junta Nacional de Auxilio Escolar y Becas, cuyo texto se adjunta a la presente resolución y se entiende incorporado, de acuerdo al siguiente nombre:

1. A.12.03.01 – Política de Respaldo de Información
2. A.12.03.01 - Procedimiento de Respaldo de Información

ARTÍCULO 2°: **PUBLÍQUESE** la presente resolución una vez tramitada, en la sección Actos y Resoluciones ubicado en el mini sitio "Gobierno Transparente", en el portal web de JUNAEB, a objeto de dar cumplimiento con lo previsto tanto en el artículo 7° de la ley N°20.285, sobre Acceso a la Información Pública, como en el artículo 51° de su Reglamento.

Junta Nacional de Auxilio Escolar y Becas
SECRETARIO GENERAL

JAIME TOHÁ LAVANDEROS
SECRETARIO GENERAL (S)
JUNTA NACIONAL DE AUXILIO ESCOLAR Y BECAS

DIRECCIÓN

MBG/RFV/FFR/jhs
DISTRIBUCION:
1. Departamentos de Dirección Nacional y Direcciones Regionales
2. Oficina de Partes

DIRECCIÓN

POLÍTICA DE RESPALDO DE INFORMACIÓN

Autorizado Firma Jefe del Informática	Autorizado Encargado de Seguridad de la Información
Elaborado por: Departamento de informática	Revisado por: Departamento de Planificación

INDICE

DIRECCIÓN

1 OBJETIVO

Asegurar la integridad y disponibilidad de la información contenida en plataformas productivas y del parque computacional de JUNAEB, mediante la configuración de operaciones de respaldo, a fin de que pueda ser recuperada ante un desastre o falla de recursos TI.

2 ÁMBITO DE APLICACIÓN

Información contenida en bases de datos relacionales, código fuentes de aplicaciones informáticas, servidores de archivos y aplicación, repositorio de archivos de usuarios críticos, mantención de equipo de usuario final, configuración de equipos de conectividad de redes de información, operativas en ambiente productivo en la plataforma tecnológica de JUNAEB y que sean de su propiedad o administrados por el Departamento de Informática.

3 ROLES Y RESPONSABLES

JEFE DEL DEPARTAMENTO DE INFORMÁTICA	Velar por el cumplimiento de la Política de Respaldo.
ENCARGADO DE UNIDAD DE SISTEMAS E INFRAESTRUCTURA	Llevar a cabo la implementación de la política de respaldos que tengan relación con servicios centralizados (infraestructura de servidores).
ENCARGADO DE UNIDAD DE SOPORTE	Llevar a cabo la implementación de la política de respaldos que tengan relación con plataforma de usuarios no centralizados.(Stand Alone)
ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN	Verificar y monitorear la ejecución de la política.

4 DEFINICIONES

Para los propósitos de esta política, las siguientes palabras se entenderán en el sentido que a continuación se indica:

Stand Alone: Se refiere a cualquier información gestionada de forma autónoma y que no sea centralizada.

Respaldos globales (full back-up): Se refiere a la operación de respaldo total del disco, en donde se obtiene una copia de la totalidad de la fuente de información y la totalidad de las operaciones que se mantienen en línea (on–line).

Respaldos parciales: Operación en que se respalda sólo una parte de la información (solamente la base de datos de una aplicación o sistema informático, una plataforma, los datos críticos o bases de datos nuevas, etc.). En este caso, las consideraciones realizadas para el respaldo global, son válidas solamente para las partes respaldadas.

Respaldos incrementales: Operación que combina respaldos globales y parciales. Se obtiene una copia de solamente las modificaciones que han ocurrido desde el último respaldo. Para realizar una recuperación se debe adicionar al último respaldo global todos los respaldos incrementales sucesivos.

DIRECCIÓN

Respaldos diferenciales: Operación similar a un respaldo incremental, en que se respaldan las modificaciones que han ocurrido desde el último respaldo global o parcial. Para realizar una recuperación se debe adicionar, al último respaldo global, solamente el último respaldo diferencial.

Respaldos Históricos: Operación de respaldo en donde se obtienen copias completas para ser almacenadas en forma histórica, conforme a los procedimientos establecidos.

Copia de Seguridad: Se refiere a copias completas de seguridad, que deben ser almacenadas en un lugar diferente al que habitualmente se mantienen los respaldos.

Recuperación: Tarea que se lleva a cabo cuando es necesario volver a un estado anterior de los datos a partir de un respaldo previamente realizado

Usuarios críticos: Personas que cumplen un rol de alta importancia en la Institución y que manejan información relevante para el desarrollo de procesos apoyados por sistemas informáticos.

Site principal: Nombre que recibe el centro de cómputo principal o Data Center, en donde residen servidores y almacenes de datos.

5 POLITICA

La presente política establece que deberán realizarse copias de respaldo de la información de:

- Repositorio de código fuentes de aplicaciones informáticas.
- Bases de datos relacionales y multidimensionales.
- Servidores de archivos y aplicación.
- Repositorio de archivos de usuarios críticos.
- Archivos del usuario final.
- Configuración de equipos de conectividad de redes de información.

5.1 PERIODICIDAD

En ámbitos críticos para la institución, se deberán almacenar al menos dos generaciones o ciclos de información de respaldo exceptuando "archivos del usuario final", para este último solo será un ciclo temporal, hasta que se realice la recepción conforme de entrega de la mantención.

Objeto de Información	Periodicidad	Tipo de respaldo	Responsable
Repositorio Código fuentes de aplicaciones informáticas	Diario	Respaldos globales (full back-up):	Unidad de Sistemas e Infraestructura
Bases de datos relacionales y multidimensionales	Según Plan de Respaldo de Base de Datos	– Respaldos globales (full back-up): – Respaldos parciales – Respaldos incrementales – Respaldos diferenciales – Respaldos Históricos – Según Plan de respaldo de base de dato.	Unidad de Sistemas e Infraestructura

DIRECCIÓN

Servidores de archivos y aplicación	Según Plan de respaldo de servidores de archivos y aplicación	– Respaldos Globales (full back-up): – Respaldos parciales – Respaldos incrementales – Respaldos diferenciales – Respaldos Históricos – Según Plan de respaldo de base de dato	Unidad de Sistemas e Infraestructura
Repositorio de archivos de usuarios críticos	Diario	– Respaldos globales (full back-up): – Respaldos diferenciales – Respaldos Históricos	Unidad de Sistemas e Infraestructura
Archivos del usuario final.	Cada vez que se realice una mantención que incluya formateo de equipo o cambio de equipo	– Respaldos globales (full back-up):	Unidad de Soporte
Configuración de equipos de conectividad de redes de información.	Cada vez que se realice un cambio.	– Respaldos globales (full back-up):	Unidad de Sistemas e Infraestructura

5.2 DISPONIBILIDAD DE INFRAESTRUCTURA

Deberá garantizarse la disponibilidad de infraestructura física y lógica adecuada de respaldo, para asegurar que éstos estén disponibles incluso después de un desastre o la falla de un dispositivo de almacenamiento.

5.3 ASEGURAMIENTO DEL RESPALDO

Cada responsable debe generar y establecer los procedimientos de prueba que aseguren la integridad de los respaldos.

5.4 UBICACIÓN

El respaldo histórico deberá almacenarse en una ubicación geográfica distinta y con un nivel mínimo de información, junto con registros exactos y completos de las copias de respaldo. Esta instalación deberá estar emplazada a una distancia tal, que escape de cualquier daño producto de un desastre en el site principal.

5.5 PROTECCIÓN FÍSICA

Los respaldos deberán cumplir con un nivel apropiado de protección física de los medios, consistente con las prácticas aplicadas en el site principal. Los medios de respaldo históricos deben tener los controles necesarios de acceso y ambientales.

Respecto de los respaldos de los archivos de usuario final, los medios que los contienen deben estar controlados por las restricciones de acceso físico de las dependencias donde se utilizan.

DIRECCIÓN

5.6 RETENCIÓN DE LOS RESPALDOS

Deberán consignarse plazos de retención de los respaldos de la institución, así como cualquier necesidad de realización de respaldos que estén permanentemente guardados, y deberán utilizarse medios y condiciones físicas de almacenamiento que garanticen una vida útil concordante con los plazos definidos.

6 REVISIÓN

El Encargado de Seguridad de la Información, efectuará una revisión de este documento al menos una vez cada 3 años desde su entrada en vigencia. Sin perjuicio de lo anterior, el documento puede ser evaluado y/o actualizado en cualquier momento, dependiendo de la necesidad de la organización por seguridad de la información.

7 DIFUSIÓN

El presente documento será difundido a través de correo electrónico y del portal de intranet institucional. Todos los usuarios de la JUNAEB, tienen la responsabilidad de conocer la presente política y cumplir lo que en ella se indica.

8 VIGENCIA

La vigencia de la presente política tendrá una duración de tres años, una vez que aprobada la resolución exenta que da origen a su entrada en vigencia.

9 CONTROL DE CAMBIOS

Nº Revisión	Cambio	Fecha	Aprobado por:
00(Cero)	Elaboración inicial	18/10/2011	Departamento de Informática
01	Actualización de la Política de Respaldo, Roles y Responsables	05-01-2016	Departamento de Informática
02	Actualización de formato.	01-07-2016	Departamento de Informática
03	Actualización de contenidos.	26-10-2016	Departamento de Informática
04	Actualización del Documento	17/11/2017	Departamento de Informática

DIRECCIÓN

PROCEDIMIENTO DE RESPALDO DE INFORMACION

Autorizado Firma Jefe del Informática	Autorizado Encargado de Seguridad de la Información
Elaborado por: Departamento de informática	Revisado por: Departamento de Planificación

INDICE

DIRECCIÓN

1 OBJETIVO

El objetivo del presente procedimiento es establecer los mecanismos y actividades que aseguren un adecuado respaldo y conservación de la información relacionada con los sistemas y operaciones de JUNAEB, teniendo en cuenta también aquella información, calificada como relevante por cada área, almacenada en los PC de aquellos funcionarios críticos de la Organización, como asimismo de las configuraciones, herramientas, software y aplicativos que operan en los servidores de JUNAEB.

Efectuar una adecuada rotulación de los medios de respaldo a fin de facilitar su identificación y relación con los sistemas. Verificar el estado de los soportes físicos que contienen las copias de seguridad, comprobando que los respaldos son capaces de recuperar la información respaldada.

2 ALCANCE

Información contenida en bases de datos relacionales, código fuentes de aplicaciones informáticas, servidores de archivos y aplicación, repositorio de archivos de usuarios críticos, mantención de equipo de usuario final, configuración de equipos de conectividad de redes de información, operativas en ambiente productivo en la plataforma tecnológica de JUNAEB y que sean de su propiedad o administrados por el Departamento de Informática.

Archivos con información de los usuarios críticos de la Institución y de los equipos que se cambian por fallos o actualización.

3 ROLES Y RESPONSABLES

RESPONSABLE	ACTIVIDAD
Jefe departamento de Informática	Implantar el procedimiento para todos los sistemas cuya operación estándar sea responsabilidad de JUNAEB. Comunicar el mismo a todas las áreas de la Organización.
Encargado de Unidad de Sistemas	Llevar a cabo la ejecución del procedimiento de respaldos de los ambientes en explotación de modo que periódicamente se realicen respaldos globales de máquinas virtuales, repositorios de archivos, discos y configuraciones de ambiente y los respaldos incrementales y/o diferenciales de los NFS y Bases de Datos según lo establecido en el plan de respaldos.
Encargado Unidad de Soporte	Realizar los respaldos de información de funcionarios críticos y de los computadores que se cambian por fallos o actualización.
Administrador de Infraestructura	Revisar periódicamente logs de respaldo de máquinas virtuales Verificar la capacidad de los discos y storage. Realizar el respaldo manual y periódico a cinta según el procedimiento de respaldo. Mantener actualizado el estado de respaldos y espacio de disco a su jefatura.
DBA	Encargado de ejecutar el plan de respaldos de las Bases de Datos, y los respaldos de sus esquemas de acuerdo a la programación descrita en el plan de respaldo.

DIRECCIÓN

4 DEFINICIONES

Para los propósitos de este procedimiento, las siguientes palabras se entenderán en el sentido que a continuación se indica:

Respaldos globales (full back-up): Se realiza un respaldo total del disco, se respalda la totalidad de las bases de datos y la totalidad de las operaciones que se mantienen en línea (on–line). La ventaja de este tipo de respaldo es que si se realiza diariamente, da la posibilidad de que ante cualquier problema de pérdida total de una máquina o base de datos, solamente se debe recuperar el respaldo del día anterior, disminuyendo la pérdida de información sólo a aquellas primeras horas anteriores a la caída. La desventaja de este tipo de respaldo es que exige contar con una gran capacidad de almacenamiento físico o TB de respaldos.

Respaldos parciales: Se respalda sólo una parte de la información (solamente una aplicación, una plataforma, los datos críticos o las bases nuevas, etc.). Como se ve, existen varios criterios para optar qué parte respaldar. Las consideraciones realizadas para el respaldo global valen aquí solamente para las partes respaldadas. La ventaja de este tipo de respaldos es que se puede obtener un respaldo de un servicio o aplicativo específico en un menor tiempo y con un requisito de capacidad de almacenamiento menor que el respaldo Full; la restauración de los respaldos también implica menos tiempo. La desventaja, por otra parte, es que al ser un respaldo puntual, aplica sólo para sistemas aislados, no se recomienda para servicios o sistemas integrados a otras plataformas.

Respaldos incrementales: Se combina con respaldos globales o parciales. Se respalda solamente las modificaciones que han ocurrido desde el último respaldo. Para realizar una recuperación se debe adicionar al último respaldo global todos los respaldos incrementales sucesivos. Es un procedimiento de respaldo ágil y que ocupa poco espacio. El procedimiento de recuperación es complejo.

Respaldos diferenciales: Similar al anterior. Se respalda las modificaciones que han ocurrido desde el último respaldo global o parcial. Para realizar una recuperación se debe adicionar al último respaldo global solamente el último respaldo diferencial. Es un procedimiento de respaldo relativamente ágil y que ocupa poco espacio, con un procedimiento de recuperación de sólo dos etapas.

Respaldos Históricos: Generación de copias "full" para ser almacenadas en forma histórica conforme a los procedimientos establecidos. Los medios magnéticos de respaldo son reutilizados luego del período de retención definido conforme hayan cumplido la vida útil definida por el fabricante.

Copia de Seguridad: Son copias "full" de seguridad que deben ser almacenadas en un lugar diferente al que habitualmente se mantienen los respaldos. Los medios magnéticos en este caso se rotan conforme la retención definida y la vida útil establecida por el fabricante.

Recuperación: Tarea que se lleva a cabo cuando es necesario volver a un estado anterior de los datos a partir de un Respaldo previamente realizado.

Usuarios críticos: Personas que cumplen un rol de alta importancia en la Institución y que manejan información relevante para el desarrollo de sus programas.

DIRECCIÓN

5 DESCRIPCIÓN DE ACTIVIDADES

Esta actividad se divide en dos, respaldos de información del Data Center y respaldos de información de estaciones de trabajo de funcionarios:

a) PROCEDIMIENTO DE RESPALDO DE INFORMACION DE DATA CENTER.

Para el respaldo de las Bases de Datos, Software, Aplicativos, Información de PC de funcionarios críticos, se aplican el siguiente procedimiento:

Plan de Respaldos

La Unidad de Sistemas e Infraestructura del Departamento de Informática, mantiene un registro denominado "Plan de Respaldo", el cual detalla los Sistemas, Bases de datos, periodicidad, tipo de respaldo, entre otros aspectos relacionados y que se ejecuta en este procedimiento. Este plan se envía al Jefe del Departamento de Informática por el Encargado de la Unidad de Sistemas e Infraestructura, el quinto día hábil del mes siguiente al revisado. La jefatura aprobará el documento, con sus comentarios y/o correcciones, entregando de vuelta una copia con lo que necesite revisarse. Los resultados de estas acciones se detallan en el próximo plan.

La documentación se guarda digitalizada en el repositorio de documentos del Departamento de Informática y, las copias de papel, en archivador destinado para estos efectos.

Para ingresar nuevos objetos al Plan de Respaldos, el Jefe de Proyecto del área de negocio dependiente del Departamento de Informática, debe registrar un requerimiento a través del Sistema de Mesa de Ayuda, conteniendo la siguiente información:

- Objeto de Información: Nombre o nomenclatura del objeto a respaldar (Base de datos, Repositorio De código fuente, Repositorio de archivos de usuario crítico, máquina virtual).
- Área de Negocio: DAE, Salud, Logística, etc.
- Sistema o fuente que respaldar: Nombre o nomenclatura del Sistema al cual pertenece el objeto.
- Jefe de Proyecto:
- Tipo de fuente a respaldar: Máquina virtual, Base de datos u otros
- Tipo de respaldo: Full, incremental.
- Programación: Diaria, mensual, semanal. Frecuencia o detalle de días.
- Horario:

El requerimiento pasará al Jefe del Departamento de Informática, para su revisión y, si corresponde, su aprobación. El Encargado de la Unidad de Sistemas e Infraestructura agregará el objeto al Plan de Respaldo y comenzará con su ejecución.

Ejecución del Plan de Respaldos

- Máquinas virtuales

Responsable: Administrador de infraestructura

Actividades:

1. Programar las tareas de copia de los objetos identificados en el Plan de Respaldos, indicando la periodicidad y destino. Para esto despliega el software Veeam Backup, disponible en la infraestructura del Data Center de JUNAEB.
2. Controlar el estado de ejecución de las tareas, utilizando las herramientas de monitoreo del software. Además, se envía a la casilla de correo electrónico respaldos_junaeb@junaeb.cl, mensajes informativos acerca de las acciones realizadas, el Administrador de Infraestructura, debe verificar que todas las tareas se desarrollen de forma satisfactoria, de no ser así, deberá volver a ejecutarlas de forma manual, el día hábil siguiente al de que se registre un error.

DIRECCIÓN

3. Controlar el espacio disponible para el almacenamiento de los respaldos tanto en el servidor de respaldo (storage lógico) como en cantidad de cintas magnéticas.
4. Catalogar las cintas magnéticas con la información, manteniendo el registro actualizado.
5. Reportar al Encargado de la Unidad de Sistemas e Infraestructura el estado de las tareas de respaldo, en forma diaria por correo electrónico.

- **Bases de datos**

Responsable: DBA

Actividades:

1. Programar las tareas de copia de los objetos identificados en el Plan de Respaldos. Para ello se utiliza un JOB (Trabajo) que incluye las instrucciones necesarias para la creación de las copias. Los respaldos se realizarán sobre los datos, esquemas, usuarios y permisos.
2. Controlar el estado de ejecución de las tareas, revisando los registros de auditoría (logs) que genera cada servidor. En caso de errores, el DBA deberá volver a ejecutar las tareas de forma manual, el día hábil siguiente al que se registre alguna anomalía.
3. Controlar el espacio disponible para el almacenamiento de los respaldos tanto en el servidor de respaldo (storage lógico) como en cantidad de cintas magnéticas.
4. Catalogar las cintas magnéticas con la información, manteniendo el registro actualizado.
5. Reportar al Encargado de la Unidad de Sistemas e Infraestructura el estado de las tareas de respaldo, en forma diaria por correo electrónico.

- **Gestión de cintas magnéticas**

Responsable: Administrador de infraestructura

Actividades:

1. Asegurar la disponibilidad/stock de cartridge de cinta magnética para la realización de traspasos de información.
2. Cambiar los cartridges de cinta magnética en las unidades robóticas dispuestas para el traspaso de información.
3. Transportar los cartridges con información, desde el Data Center de JUNAEB hasta el Edificio Institucional. Además, almacena los artículos en forma ordenada y segura, etiquetada de acuerdo a la información que los identifica en el catálogo, en un espacio controlado con medidas de control de acceso y ambiental.
Controlar y gestionar el catálogo de cintas, que se encuentra en el software Veeam Backup. La información contenida se enviará en forma mensual en conjunto con las actividades del Plan de Respaldos.

6. PROCEDIMIENTO DE RESPALDO DE ESTACIONES DE TRABAJO DE FUNCIONARIOS.

a) PROCEDIMIENTO DE RESPALDO EN MANTENCIÓN DE EQUIPOS.

La Unidad de Soporte mantiene el registro de usuarios críticos de la Institución, actualizada cada tres meses, mediante el envío de correo electrónico al Jefe de los Departamentos, quienes validarán los nombres y realizarán las modificaciones que estimen convenientes. Cuando un funcionario salga de la lista de críticos, la función de respaldo de sus archivos se desactivará y su información pasará a cinta magnética para almacenamiento por espacio de 5 años.

Este respaldo aplica solo a los funcionarios que son declarados como críticos, cuya calidad es definida por la Jefatura del Departamento del cual dependen. Se actualiza a demanda y se mantiene una copia con la fecha de la última actualización en el directorio compartido:

En los computadores y notebooks asignados a los funcionarios críticos se realizarán las siguientes tareas:

Se respaldará la carpeta "Mis Documentos" del usuario, excluyendo archivos de imagen, música y videos. Si por la naturaleza de la información es necesario guardar los formatos excluidos, la Jefatura deberá justificar su inclusión.

DIRECCIÓN

Se instalará el software Cobian Backup, en su última versión, que puede descargarse desde internet. Este programa es gratuito y libre de licenciamiento o mantención. La instalación se realiza de manera normal, solo siendo necesario en este paso elegir dos alternativas:

- Iniciar como aplicación
- Iniciar el servicio de copia en segundo plano

Se programará una tarea de respaldo con el nombre de "Archivos", la cual deberá contener:

- Tipo de respaldo: Incremental
- Fuente: Carpeta "Mis Documentos", del funcionario.
- Destino: Carpeta "RespaldosCriticos".
- Horario: Definidos en nómina de funcionarios críticos. No deberá programarse a la misma hora de otros funcionarios. De Lunes a Viernes.
- Dinámica: Prioridad normal. Copias completas a guardar 1. Hace un respaldo completo cada 10 incrementales.
- Filtros: Excluir los ficheros por máscara, esto es, *.mp3, *.jpg, *.wma, entre otros.
- Atributos avanzados: Seleccionar "Borrar carpetas vacías".

Dentro de la aplicación Cobian, también deberá configurarse las opciones:

- Correo: Establecer los parámetros para el envío de correo electrónico como sigue:
- Nombre del remitente: Cobian "Nombre del usuario"
- Dirección del remitente: notificaciones@junaeb.cl
- Servidor de SMTP: smtp.junaeb.local
- Asunto: "Cobian (%COMPUTERNAME)
- Destinatarios: respaldospc@junaeb.cl
- Diario: Establecer la configuración para el reporte diario:
- Registro normal.
- Opciones de diario: Crear un nuevo fichero de diario cada día.
- Borrar ficheros de diario más viejos que (días): 30
- Enviar diario, enviar como anexo, enviar sólo si hay errores y borrar si es enviado correctamente.
- Cuando enviar: Enviar diariamente, a las 13:00:00.

b) PROCEDIMIENTO DE RESPALDO EN MANTENCIÓN DE EQUIPOS.

En el caso de que de los computadores sean sometidos a procedimientos de mantención, esto es, traspaso de información desde un equipo a otro, a raíz de reemplazo de equipo por obsolescencia o por mal funcionamiento, ejecutando las siguientes tareas:

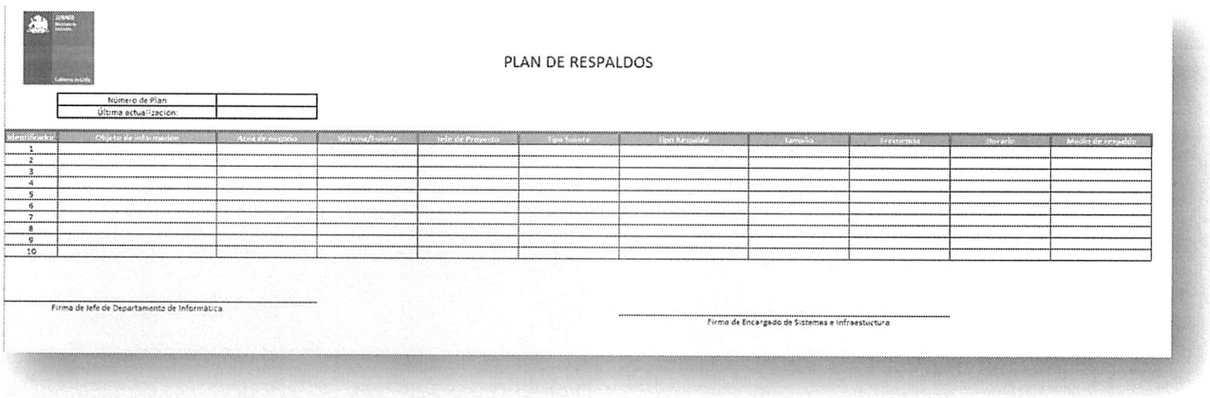
- Se quitará el o los discos duros del equipo actual y se conectarán al equipo de reemplazo para el traspaso total de los datos.
- Los discos se etiquetarán en su superficie, indicando:
- Nombre del funcionario.
- Fecha de permanencia, esto es, hasta qué fecha de guardará en la caja de "Respaldos Transitorios" ubicada en bodega de la Unidad de Soporte.
- Se ingresarán los números de serie de los discos y su fecha de permanencia en la Ficha de Mantención de Discos Duros, disponible en el Sistema de Gestión de Inventario.

DIRECCIÓN

Se entregará el nuevo computador al funcionario asignado a través del Sistema de Gestión de Inventario, en donde se indica que los datos almacenados en el computador anterior, permanecerán en custodia en la Unidad de Soporte hasta la fecha indicada, y luego de eso serán eliminados de manera definitiva.

6. REGISTROS

- Planilla registro "Plan de Respaldos".



PLAN DE RESPALDOS

Numero de Plan	
Última actualización:	

Identificador	Objeto de respaldo	Área de negocio	Responsable	Jefe de Proyecto	Tipo Inicio	Tipo Respaldo	Tamaño	Frecuencia	Horario	Medio de respaldo
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										

Firma de Jefe de Departamento de Informática

Firma de Encargado de Sistemas e Infraestuctura

Fuente propia: Departamento de Informática

7. DIFUSIÓN

El presente documento será difundido a través de correo electrónico y del portal de intranet Institucional. Todos los usuarios de la JUNAEB, tienen la responsabilidad de conocer el presente procedimiento y cumplir lo que en ella se indica.

8. REVISIÓN

El Encargado de Seguridad de la Información, efectuará una revisión de este documento al menos una vez cada 3 años desde su entrada en vigencia. Sin perjuicio de lo anterior, el documento puede ser evaluado y/o actualizado en cualquier momento, dependiendo de la necesidad de la organización por seguridad de la información.

9. VIGENCIA

La vigencia de la presente política tendrá una duración de tres años, una vez que aprobada la resolución exenta que da origen a su entrada en vigencia.

10. CONTROL DE CAMBIOS

Nº Revisión	Cambio	Fecha	Aprobado por:
00(Cero)	Elaboración inicial	18/10/2011	Jefe Departamento Informática
01	Actualización de la Política de Respaldo, Roles y Responsables	05-01-2016	Jefe Departamento Informática
02	Actualización de formato	01-07-2016	Jefe Departamento Informática
03	Actualización de formato, y procedimiento completo	10-11-2017	Jefe Departamento Informática

DIRECCIÓN