Políticas de Backup

Oficina Nacional de Contrataciones

Versión 3

Mayo 2021

I. Introducción

El presente documento tiene como fin describir las políticas de backup que se deben implementar, para resguardo y recuperación de la información y los sistemas de la Oficina Nacional de Contrataciones (ONC).

Se describen aquí los diferentes tipos y almacenamientos de *backup* (servidores, cintas y *storage*), momentos de ejecución, manejo de los datos y políticas de recuperación.

II. Alcance

Aplica a los datos ubicados en servidores y *storage* bajo resguardo del área de infraestructura y datos que los desarrolladores o el administrador de servidores incluyan por pedido expreso en algún plan de backup brindado por el área.

III. Responsabilidad

La responsabilidad de almacenamiento abarca únicamente a los datos contenidos en los servidores y *storage* ubicados y administrados por el Centro de Datos de la Subsecretaría de Innovación Administrativa. La mencionada Subsecretaría no tiene responsabilidad sobre documentos en computadoras, servidores o dispositivos de almacenamiento por fuera de este centro de datos o bien por archivos ubicados en las computadoras personales o de escritorio de este organismo, sí de todos los documentos relacionados con los Sistemas de Compras del Estado: Compr.AR, Contrat.Ar como todos sus sistemas derivados generados a través de los sistemas alojados.

Tampoco se realizan backups de equipamiento correspondiente a organismos descentralizados o externos que no fueran pedidos mediante solicitudes formales. Excepción a esta regla será cuando el modo de operación de los servicios informáticos de la ONC frente a organismos sea provisto a través de un

servicio de hosting o housing que la ONC disponga, en cuyo caso deberán realizarse los backups acorde a la presente política.

Esto se aplica a los componentes de los sistemas acordAR, ContratAR, ComprAR, SubastAR, Sipro, Trámites Express, SiByS, PAC, Registro de Constructores de la ONC y Bienes Patrimoniales del Estado.

La Oficina Nacional de Contrataciones (ONC) es la responsable de confeccionar las políticas referidas al almacenamiento y aseguramiento de la información de los componentes mencionados. La Dirección Nacional de Sistemas de Administración y Firma Digital (DNSAFD) – o la que en el futuro la reemplace- , perteneciente a la Subsecretaría de Innovación Administrativa (SSGA), siendo el área responsable de la administración de los servidores y dispositivos de almacenamiento (storage) de la ONC, deberá adecuar los procedimientos referidos al almacenamiento primario del backup incluyendo las bases de datos, el almacenamiento y procesamiento de los archivos e información y el hospedaje de los sistemas y componentes, para que los mismos se encuentren acordes a la presente política y a sus propias capacidades.

IV. Archivos que se almacenan en copias de respaldo

Debe realizarse un respaldo de los archivos que se incluyan en alguno de estos puntos:

1. Servidor completo incluyendo sistema operativo, en caso de servidores virtuales.
2. Archivos de configuraciones, documentos, base de datos y archivo de usuarios compartidos.
3. Todos los tipos de archivos ubicado en storage que contengan la funcionabilidad de Tipo de backup en snapshot (STORAGE DE ALMACENAMIENTO TIPO NAS)

4. Todo los dumps de BBDD, archivos de configuración, archivos que almacenen el aplicativo como por ejemplo PDFs.

ACLARACION:

Los archivos antes descriptos deben tener copias de seguridad con los sistemas o plataformas que defina el área de infraestructura, tomando como referencias, backup a cinta/tape, backup a disco**.**

- Un snapshot es una foto de los datos que se almacenan en el storage en un momento específico en el tiempo.
- Un snapshot hace referencia a un directorio en el storage, incluidos todos los datos almacenados en el directorio y sus subdirectorios. Si se modifican los datos a los que hace referencia un snapshot, el snapshot almacena una copia física de los datos que se modificaron.
- Los snapshot se crean de acuerdo con las especificaciones dadas o las establecidas y las genera automáticamente para facilitar las operaciones del sistema.
- Estas instantáneas se eliminan automáticamente cuando el storage ya no las necesita por antigüedad o funcionabilidad.
- Los snapshot utilizan una parte del storage, donde se guardan los datos/archivos productivos.
- No se almacenan en otro espacio diferente a producción.
- Su capacidad es limitada al espacio que tengamos disponible en el almacenamiento.
- Por rotura de equipo se puede tener pérdida total o parcial de datos.

Consideraciones Adicionales

A fines de realizar los respaldos y garantizar la disponibilidad de la información, todos los datos considerados críticos para la ONC no deberán ser almacenados

en computadores, servidores y/o dispositivos que se encuentren fuera del Centro de Datos, con excepción de los medios utilizados para almacenar dichos respaldos de forma externa a la oficina.

V. Criterio de elección para la gestión de software de backup

Para seleccionar el tipo de backup a realizar se evalúan los siguientes criterios:

1. Si el servidor es de tipo físico o virtual
2. Tipo de sistema a reguardar (Ej. Web, App, Base de Datos, etc).
3. Volumen de la información a resguardar.
4. Volumen de almacenamiento disponible en los sistemas de backup.
5. Frecuencia del resguardo
6. Nivel de Criticidad (Alta, Media, Baja)
7. Periodicidad y Retención (Mantenimiento en el tiempo)

La gestión y selección del software de backup debe ser elegida por el área de infraestructura que tiene a cargo las políticas y lineamientos correspondientes y su cumplimiento.

En casos que no se disponga del software o método adecuado para el respaldo necesario se deberá implementar un sistema para confeccionar estas necesidades.

Metodología o procedimiento general de resguardo

- Siempre que sea posible el resguardo se hace de las siguientes maneras. Todos los días se hacen backup full e incrementales en los horarios de 8

pm a 8 am, en las herramientas de backup para servidores virtuales y a cinta. (Ver documentos con políticas de backup y retención en los anexos de cada tipo de gestión).

- En el caso del Tipo de backup en snapshot el almacenamiento máximo corresponde a los últimos 7 días.

EJEMPLOS

Bajo estas consideraciones se podrá recuperar una versión particular, además de las versiones completas según el sistema de backup.

- De una semana atrás para el backup tipo snapshot en los storage.
- En el backup tipo servidor:
    - Servidor desarrollo: 1 mes
    - Servidor producción 2 meses
- De 6 meses para atrás en el backup de tipo cinta.

CONSIDERACIONES

- Para ver tiempos de retención y políticas deberá acceder a los documentos anexos de backup de tipo servidor y tipo cinta.
- En el caso de los snapshot el máximo es una semana para todos los archivos.
- Se podrá recuperar versiones particulares, de la última semana y versiones completas.
- Ante perdida de datos se podrá acudir a backups diferenciales y respaldos full.

VI. Procedimiento de restauración

La restauración se realiza en el servidor o lugar original dependiendo del tamaño.

Ante perdida de información se deberá solicitar lo antes posible, ya que de transcurrir mucho tiempo el rehusó de los volúmenes de almacenamiento se puede sobrescribir.

VII. Ambiente de Guarda

Las copias de seguridad deberán estar almacenadas en un ambiente específico adecuado en seguridad perimetral, climatización, infraestructura y protección necesaria para la preservación en el tiempo de los dispositivos físicos contenedores de datos de los resguardos o de los medios utilizados para el respaldo de la información.

VIII. Rutinas de seguimiento

La información en los diferentes tipos de backup se controla diariamente mediante los softwares de gestión para validar su correcta ejecución. Sin embargo, no se realizan tareas de restauración a excepción de pedidos explícitos.

Las pruebas que se realizan por pedidos explícitos consisten en recuperar servidores desde la plataforma, recuperar archivos desde la cinta y recuperar archivos desde un snapshot.

IX. Protección ante perdidas

Los respaldos de los datos considerados críticos para la ONC deberán ser cifrados con protocolos suficientemente robustos (AES-254, RSA, o superior) para permitir garantizar la confiabilidad y protección ante eventual robo de estos mismos.

X. Pruebas periódicas

La presente política propone un esquema de pruebas periódicas para la verificación de los respaldos con el fin de llevar una bitácora de los mismos, garantizar la salud de los medios utilizados y correcta creación tanto de los respaldos y recuperación de los mismo. Así mismo, es recomendable que estas pruebas se deberán realizar en un ambiente separado, bien definido y delimitado, dentro de un Centro de Datos o infraestructura específica a tal fin, con la mayor similitud posible a la infraestructura de producción posible.

La periodicidad de las pruebas deberá ser como máximo de 12 meses o bien realizarse en caso de cambios estructurales, de arquitectura o infraestructura que puedan afectar el proceso de restauración. El RESPONSABLE deberá registrar dichas pruebas con fecha, hora y evidencia de los resultados de restauración. Esta bitácora deberá ser validada y certificada por el área responsable del sistema correspondiente a la Oficina Nacional de Contrataciones.

XI. Posibles pérdidas de datos

La presente política tiene como límite para una posible pérdida de datos los siguientes casos:

- Rotura de servidores de gestión de backup por negligencia, falla de sistema o hardware.
- Perdida de los resguardos en el archivo en el sistema de almacenamiento o volumen donde se realizan, por falla de sistema, hardware o negligencia.
- Perdida de datos en los sistemas magnéticos.
- Daño total de los datacenter o lugar de almacenamiento.

Esquema de backup modelo para la solución

Ambiente de backup.

Data Set/Tipo de datos a respaldar	Capacidad de un Backup Full (TB)	Backups Full por semana	Backups Incre-mental por Semana **	Tasa de cambios diarios	Tasa de crecimiento Anual	Tiempo esperado para recuperación (RTO)	Retención
File System ***(ejemplo)***	*1,5*	*1*	*5*	*1%*	*10%*	*1 hora*	*1 anual x 10 años* *12 mensuales por 1 año (el último)* *30 diarios x 1 mes (el último)l*
File System Windows		1	7	*Sin datos*	*20%*	*24hs*	*1 anual x 10 años* *12 mensuales por 1 año (el último)* *30 diarios x 1 mes (el último)*
Virtual Machines Production		1	7	*1 %*	*20%*	*2 hs*	*1 anual x 10 años* *12 mensuales por 1 año (el último)* *30 diarios x 1 mes (el último)*
Virtual Machines Production-critico		1	7	*1 %*	*20%*	*2 hs*	*1 anual x 10 años* *12 mensuales por 1 año (el último)* *30 diarios x 1 mes (el último)*
Virtual Machines Preproduction		1	5	*0,2 %*	*20%*	24 hs	*6 mensuales por 1 año (los 6 últimos)* *4 semanales x 1 mes (el último)*
Virtual Machines TEST		1	*5*	*0,2 %*	*20%*	*24 hs*	*6 mensuales por 1 año (los 6 últimos)* *4 semanales x 1 mes (el último)*

Virtual Machines DESA		1	*5*	*0,2 %*	*20%*	*24 hs*	*6 mensuales por 1 año (los 6 últimos)* *4 semanales x 1 mes (el último)l*
Datos No Estructurados (imagenes, videos, etc.)		1	7	1 %	*20%*	24 hs	*1 anual x 10 años* *12 mensuales por 1 año (el último)* *30 diarios x 1 mes (el último)l*
Total		-	-				

Nota: Se considera semana de 5 días a los días de lunes a viernes y semana de 7 días a los días de lunes a domingo. La selección de frecuencia se hará en función a la tabla detallada previamente.

Esquema del Backup	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
Ventana de Backup (en horas)	12 hs	12 hs	12 hs	12 hs	12 hs	24hs	24hs
Hora inicio del Backup (00:00-24:00)	20:00	20:00	20:00	20:00	20:00	00:00	00:00

¿Encripta o comprime sus backups?	Nosotros no comprimimos y encriptamos los backups

Por favor agregue toda información que considere nos pueda ayudar a entender con más detalle su ambiente (cuestiones a resolver, diagrama de red de la arquitectura de backup, etc.)

Se deja un anexo 1 sobre un procedimiento para una política de backup a cinta.

XII. ANEXO 1: Política de BackUp a Cinta

A. Objeto:

Establecer pautas para el resguardo, mantenimiento y control de la información.

B. Alcance:

Desde la administración y gestión de las copias de resguardo de información, registración de las mismas, responsables de la concreción y control, hasta el posterior traslado de los dispositivos de almacenamiento para su resguardo.

C. Definiciones y Abreviaturas:

organismo: JGM

dependencia: ONC

TDC: Centro de Cómputo/infraestructura.

SGI: Sistema de Gestión de Incidencias

CR: Centro de Respaldo.

Lote: el conjunto de cintas de backups o resguardo obtenidas de todos los equipos (servidores), que prestan servicio en el datacenter del Edificio del ORGANISMO en un día.

Fecha del backup o resguardo: la que corresponde al día de trabajo que será resguardada, que no necesariamente es la fecha del día en que se ejecuta el “proceso de backup o resguardo”. Es decir que, si el backup se realiza antes de las 0 horas, la fecha de backup corresponde al día de la fecha; si se ejecuta después de las 0 horas y

como límite máximo hasta las 9 horas (a.m.), el backup corresponde a la información del día anterior.

D. Documentos de Referencia:

- PE-XXX-T-0n-Autorización Traslado Medios y Acceso Sitios (Medios: dispositivos de almacenamiento)

E. Responsabilidades:

1. Responsables de cumplimiento

Son responsables del cumplimiento del presente procedimiento las personas que se desempeñen en el Área TDC de la dependencia.

2. Responsables de actualización

El responsable de la actualización del presente procedimiento es el área de TDC. La responsabilidad de las personas que integran dicha área es la de revisar y actualizar en caso de que corresponda, el presente documento de acuerdo al esquema de revisión y actualización establecido y a las solicitudes efectuadas por las diferentes personas u organismos que se encuentran involucrados.

El plazo máximo para la revisión del presente documento será como máximos 3 años y se deberán tener en cuenta las siguientes tareas.

- Analizar las métricas de consumo de los backups vigentes y ajustar el dimensionamiento y escalamiento.
- Realizar los cambios correspondientes a modificaciones de arquitectura y componentes.

- Validar las responsabilidades y e impactar los cambios si la estructura del mapa del estado fuere modificada o bien así las responsabilidades de cada área.
- Revisar el documento, completar y ajustar acorde a las tecnologías vigentes.
- Mejorar y optimizar en los procedimientos existentes para optimizar el espacio y los recursos asignados.
- Corroborar el cumplimiento de la política.

F. Desarrollo:

1. Administración y rotulado de las cintas de resguardo

Para asegurar una administración homogénea, ordenada y continua de las cintas que se utilizan para los resguardos de los datos, aplicaciones y software residente en los servidores, se describe a continuación el ciclo de administración de las mismas.

Las cintas se asignan de la siguiente forma:

- Lote 1: todas las cintas del backup del lunes
- Lote 2: todas las cintas del backup del martes
- Lote 3: todas las cintas del backup del miércoles
- Lote 4: todas las cintas del backup del jueves
- Lote 5: todas las cintas del backup del primer viernes del mes (semanal)
- Lote 6: todas las cintas del backup del segundo viernes del mes (semanal)
- Lote 7: todas las cintas del backup del tercer viernes del mes (semanal)
- Si el mes tiene cinco viernes, se genera el Lote 8 que lo conformarán las cintas del cuarto viernes del mes (semanal)
- Lote Enero, Febrero,..., Diciembre: todas las cintas del backup del último viernes del mes correspondiente, backup mensual.

Lotes 5/6/7/8: Backups Semanales, Lotes **5, 6, 7 y 8** (Lote 8 para el caso que el mes tenga 5 viernes)

A modo de ejemplo se presenta esta matriz, donde se indican los distintos lotes de cintas asignados para resguardos durante un mes.

	Lunes	Martes	Miércoles	Jueves	Viernes
Semana 1	Lote 1	Lote 2	Lote 3	Lote 4	**5- Semanal**
Semana 2	Lote 1	Lote 2	Lote 3	Lote 4	**6-Semanal**
Semana 3	Lote 1	Lote 2	Lote 3	Lote 4	**7-Semanal**
Semana 4	Lote 1	Lote 2	Lote 3	Lote 4	**8-Semanal**
Semana 5	Lote 1	Lote 2	Lote 3	Lote 4	**Mensual**

Forma de etiquetar las cintas.

Las cintas deben etiquetarse con la siguiente información:

Lote Nro :	Mensual/Semanal/Diario	
Equipo :	Cinta Nro:	ID:

Lote Nro: numeración de 1 a 8 inclusive.

Mensual/Semanal/Diario: Se debe especificar la frecuencia de uso.

Equipo: nombre del servidor, del cual se efectuó el resguardo de la información.

Cinta Nro: Para el caso que se requiera más de un backup para un mismo equipo, la nomenclatura adaptada sería: 1/2 y 2/2, por ejemplo, esto se interpreta

de la siguiente forma: el backup de dicho equipo esta compuesto por 2 cintas en total, “número de cinta/cantidad total de cintas utilizadas” y así sucesivamente.

ID Cinta: Para saber qué cinta se utilizó y poder llevar un control de reutilización de la misma. Este valor es de tipo numérico y es asignado consecutivamente.

2. Registro/Control del resguardo, uso de cintas

Para efectuar un control de los resguardos realizados, donde figure la relación lote-día de la semana, qué cintas se utilizaron y cuántas veces, etc. se genera una planilla (listado) que contiene la siguiente información de la conformación de los Lote 1 a Lote 8 y Lotes mensuales.

En la planilla hay una “solapa” asignada a cada lote de cintas de acuerdo al esquema indicado inicialmente en este procedimiento, donde figura la siguiente información, que se muestra solo modo de ejemplo:

Lote 3											
Día: Miércoles			**Fecha Backup:** *dd/mm/yyyy*								
Equipo	Tipo de Cinta	Tipo Backup	Id Cinta	Reutilización Nº	Total Cintas	Status de Cinta	Status de Log	Cinta Seleccionada para llevar al BNA	Verificación de Etiquetas de Cintas	Valor Status	Reuso base
Servidor 1	DDS3	FULL	2571	**6**	1	Correcto	Correcto	SI		2	-149
Servidor 2	DDS3	FULL	2519	**72**	1	Correcto	Correcto	SI		2	-83
Servidor 3	LTO3	FULL	2546	**57**	1	Correcto	Correcto	SI		2	-98
Servidor 4	DDS4	FULL	2538	**62**	1	Correcto	Correcto	SI		2	-93
Blade 1	DDS4	FULL	2521	**69**	1	Correcto	Correcto	SI		2	-86

Blade 2	LTO3	DIF	2429	**18**	1	Correcto	Correcto	SI		2	-49
Blade nn	LTO3	DIF	2552	**48**	1	Correcto	Correcto	SI		2	-107
Total Cintas					**9**						

Cada fila pertenece a un tipo de backup o resguardo para un equipo. El significado de cada columna es el siguiente:

- **Equipo:** nombre del equipo al cual se le realiza el resguardo de información.
- **Tipo Cinta:** formato del dispositivo que se usa para el backup (DDS3, DLT4, LTO8; etc.)
- **Tipo Backup:** Incremental, Diferencial y/o Full.
- **Id Cinta:** número que identifica unívocamente a una cinta, que forma parte de un lote.
- **Reutilización Nro:** cantidad de veces que se usó la misma cinta, para realizar tareas de resguardo.
- **Total Cintas:** cantidad de cintas que utiliza el equipo.
- **Status de la Cinta:** celda de actualización automática que cambia de “Correcto” a “Cambiar Cinta” cuando el nro de reutilizaciones supera 80.
- **Status del Log:** a completar por el Operador indicando cualquier novedad encontrada durante la revisión de los logs del backup
- **Cinta Seleccionada para llevar al CR:** indica si la cinta ha sido seleccionada para ser trasladada al Centro de Respaldo**.**
- **Verificación de Etiquetas de Cintas:** Está columna la registra el Encargado de llevar las cintas al CR, valores posibles: tilde (ok), raya (no ok).
- **Valor Status:** celda de actualización automática que cambia de “2” a “1” cuando el nro de reutilizaciones supera 80.
- **Reuso base:** utilizado para calcular la cantidad de usos de las cintas. Cuando se incorpora una cinta nueva, se debe introducir un valor tal, que el resultado indicado en la celda Reutilización Nro: de la misma fila sea cero.

3. Registración de la operación de resguardo

Es tarea del Operador de Resguardo, registrar sobre el documento propuesto, lo siguiente:

Lote anterior

Status de Log: Verificar los logs de cada trabajo programado Job y luego registrar sobre la solapa correspondiente en la columna denominada “Status de Log”, su resultado. Si el resultado fue satisfactorio entonces registrar “correcto”, en caso contrario colocar en el mismo campo la razón (incorrecta).

Status de Cinta: registra el estado de la cinta, si corresponde el estado “Correcto” o “Cambiar Cinta”, de acuerdo al Log de dicho trabajo de resguardo. Para registrar dicho estado se ha estipulado: 2 (Correcto), en caso contrario 1 (Cambiar Cinta) en la columna denominada **Valor Status**, este valor depende del resultado del Status del Log, el número máximo de reutilización de la cinta y/o si la misma sufrió algún daño físico.

Reutilización Nº: Sumar uno al último número que figura como **“Nro”** como identificador de reutilización de las cintas.

Cinta Seleccionada para llevar al CR: en esta columna se registra si la cinta utilizada para realizar el resguardo, es apta para ser llevada luego al CR.

Por último, si todos los campos, están correctos y completos, imprimir una copia del informe y firmarla. La copia impresa del informe es guardada por el Operador de Resguardo, en un archivo destino para tal fin.

Lote Actual

Revisar que estén todos los resguardos realizados (del día anterior), como así también su correspondiente registración, antes de comenzar a registrar el lote actual a ser procesado.

Ubicar la solapa de acuerdo al día de la semana.

Fecha Backup: completar la fecha que corresponde al resguardo

En caso de que haya que reemplazar una cinta por pérdida, rotura o desgaste, la nueva cinta se identifica con un nuevo **Id**.

Luego de obtener el **Id** correspondiente y de haber completado la Etiqueta de la nueva cinta, el Operador debe completar la fila correspondiente, en el documento propuesto, en la solapa correspondiente de dicho lote a ser procesado.

Se ha estipulado que el máximo número de reutilización de una misma cinta es de: **80** (ochenta) veces o la que el fabricante indique en el producto, al llegar al número antes mencionado, dicha cinta debe ser reemplazada.

Nota: Los pasos mencionados con anterioridad (6.2 y 6.3), se pueden aplicar a la metodología de trabajo de resguardo de la información de los Sistemas Operativos de los servidores, como así también de los resguardos (semestrales) de los archivos tipo Logs de los backups y eventos. Dicha información puede ser registrada en la planilla.

Las copias de resguardo de los Sistemas Operativos deben guardarse como se indica en el punto 6.4, ítems: 1 al 4, inclusive. Con la salvedad que la registración será semanal, mientras que las cintas que se obtengan de los backup semestrales de los logs de backup y de los eventos, se deben trasladar al CR, junto con los resguardos de tipo mensual.

Baja y posterior destrucción de Cintas

La cinta que es desafectada por: pérdida, rotura o desgaste, debe ser registrada por el Operador de Resguardo en el documento en la solapa denominada "**Cintas de Baja",** donde se registran los siguientes datos: Fecha de la baja, Id de la cinta, Lote del cual se extrae, motivo de la baja, y nombre del equipo que resguardaba.

Una vez cada 360 días el Operador de Resguardo realiza la tarea de destrucción de cada una de las cintas registradas en la planilla antes mencionada, aplicando golpes y/o cortes (con ayuda de una herramienta adecuada para tal fin) sobre las mismas, para que de esta forma se obtengan secciones más pequeñas. La destrucción parcial de las cintas se lleva a cabo en las instalaciones que posee el área de operaciones (depósito), utilizando para esto elementos de protección personal (máscaras respiratorias, guantes descartables y protección ocular).

Luego de realizar las acciones que sean necesarias, el material sobrante se deposita en bolsas de residuos debidamente etiquetadas.

Dicha etiqueta debe contener, como mínimo: nombre y apellido de la persona que efectúa la operación, firma del mismo, fecha de corte, como así también la firma del Responsable de Seguridad Informática.

Se debe dejar una copia del registro (con todos los campos completos) antes mencionado, en una carpeta destinada para tal fin, para su verificación posterior.

Luego de realizar estas tareas, el Operador de Resguardo, registra la fecha de destrucción en la columna correspondiente denominada "Fecha de destrucción parcial", en el documento para este fin.

En caso de que no pueda concretarse alguna de las tareas de destrucción (debido a, pero no restringido a estos ejemplos: falta de medios, falta de presupuesto para reemplazo de medios), se deberá dejar registro de la no

destrucción de medios en el mismo documento indicado anteriormente (LT-TDC-T-nn).

El último paso es el de registrar sobre el documento LT-TDC-T-nn Planilla de Inventario de Cintas en la columna "**Fecha de Entrega-Destrucción Total**". El Operador de Resguardo deberá hacer entrega a un servicio público a cargo de destrucción segura de datos o en caso de no disponibilidad de dichos servicios el Operador de Resguardo entregará los residuos restantes para su desecho final asegurando la entrega un proveedor dedicado a tal fin que deberá garantizar mediante un acuerdo de confidencialidad la no restauración, recuperación, divulgación ni explotación de los datos de los residuos hasta la destrucción total de los mismo.

Este Documento, proporcionado, se debe archivar junto a una etiqueta que dio origen a dicha acción, en la carpeta destinada a tal fin.

Altas, bajas y modificaciones:

Cualquier modificación que sea necesario realizar en la planilla descripta en "6.2 Registro/Control del resguardo, uso de cintas", como, por ejemplo, pero no restringido a:

- Agregar un equipo para toma de BackUp
- Eliminar un equipo de la toma de BackUp
- Modificar el nombre de un equipo en la planilla
- Suspender provisoriamente la toma de un BackUp
- Suspender definitivamente la toma de un BackUp
- Reanudar la toma de un Backup que hubiera sido suspendido provisoriamente

Debe ser solicitada mediante el envío de un SGI dirigido al Área TDC, indicando Nombre del Equipo, Acción a Tomar y fecha a partir de la cual aplica la solicitud.

El personal del Area del TDC debe documentar lo solicitado completando los datos requeridos (“Fecha”, “Descripción de la Novedad” y “SGR Asociado”) en la solapa “novedades” de la planilla.

4. Guardado de las cintas de Backups en línea

Las cintas en línea se guardan en:

1) En área de seguridad del CR, juego completo de la operación de backup de dos días anteriores (como ejemplo, podemos citar que siendo hoy Lunes, se guardan las cintas del día jueves).

El ciclo diario es el siguiente:

El Operador de Resguardo:

1. Realizar la registración y control diario de las operaciones de resguardo. Punto 6.3
2. Luego, retira las llaves de la caja fuerte del panel de llaves ubicado en la Oficina de Seguridad Informática.
3. Retira las cintas de resguardo o backup de los equipos ubicados en el TDC.
4. Lleva el Lote de cintas desde el TDC a la caja fuerte del TDC.
5. Retira de la caja fuerte las cintas del lote del día actual o corriente y las lleva y ubica en los equipos para el próximo backup o resguardo.
6. Prepara el lote de cintas del backup correspondiente a dos días anteriores para ser trasladado área de seguridad del CR (ejemplo citado precedentemente punto a), de acuerdo a la hoja impresa del documento acordado

El Encargado de llevar las cintas al CR:

1. Busca y/o coordina con el Operador de Resguardo, la documentación necesaria para poder controlar las cintas que son trasladas al CR.

2. Luego, retira las llaves de la caja fuerte del panel de llaves de la Oficina de Seguridad Informática, para abrir la caja fuerte del TDC.
3. Extrae de la caja fuerte el Lote de cintas asignado y preparado para el CR, revisa que esté de acuerdo con lo definido en la planilla que completó el Operador de Resguardo. Si detecta alguna anomalía o discrepancia se comunicará con el Operador de Resguardo, quien determina los pasos a seguir y hace entrega de los documentos de control sin firmar. Si el control es satisfactorio entrega la documentación de control al Operador de Resguardo, firmada. *(en los casos en que, por algún motivo, se omita la firma y siendo el control positivo por parte del Encargado de llevar las cintas, se registra el motivo o razón).*
4. Pasada esta instancia, retira las cintas.
5. Deposita las cintas en el CR y trae el lote que estaba guardado de la vez anterior.
6. Guarda el Lote que trasladó desde el CR, en la caja fuerte del TDC.
7. Por último, deja la llave de la caja fuerte, en el tablero de llaves de la Oficina de Seguridad Informática.

5. Respaldo de las cintas de backups históricos

Todos los meses, una vez realizado el backup o resguardo mensual del mes en curso (última semana de dicho mes), se guarda y traslada al CR como histórico, el Lote de cintas del backup mensual que contemple *dos meses anteriores con respecto al mes en curso,* es decir si se extraen las cintas del mes de Octubre, se deben resguardar las cintas del mes de Agosto y así sucesivamente. Mientras tanto el backup mensual del mes en curso es retenido en el TDC del ORGANISMO, hasta tanto se cumpla el término de dos meses, para ser trasladado.

La copia de resguardo histórico se conserva en el CR, en un armario destinado a tal fin.

Las tareas para el traslado son las siguientes:

1. El Operador de Resguardo avisa al Área nnnn con copia al Encargado de trasladar las cintas al CR, que se realiza la operación de resguardo mensual del mes en curso, dando lugar al traslado de las cintas del backup o resguardo mensual de dos meses anteriores.
2. El Operador de Resguardo Hace entrega de una copia **(firmada por éste)** al Encargado de traslado. La entrega se realiza de forma impresa con los registros correspondientes al mes de resguardo que se llevan al CR, para su posterior control.
3. El Encargado del traslado acuerda con el Coordinador del CR, día y hora para que se trasladen a esta oficina las cintas de resguardo históricas.
4. Se traslada al TDC y extrae el Lote de cintas del backup histórico, las cuales se encuentran preparadas para ser llevadas y realiza un control de las cintas preparadas versus el documento que le proporcionó el Operador de Resguardo mencionado en el **punto 2**. Si el control es satisfactorio entonces el Encargado de Traslado debe **firmar el documento**, si no, debe coordinar con el Operador de Resguardo los pasos a seguir y no firma la hoja, hasta tanto se solucione el desvío.
5. Se traslada al CR donde extrae las cintas que contiene el resguardo mensual (de dos meses atrás) y las coloca en el armario destinado a tal efecto.
6. Previamente el Encargado del Traslado, debe extraer las cintas del corriente mes y del año anterior, las cuales deben ser Identificadas por sus etiquetas.
7. Luego de realizar estas dos tareas antes mencionadas, el Encargado de Traslado entrega las cintas extraídas al Operador de Resguardo, para que realice el resguardo mensual.
8. El Operador de Resguardo, controla el estado físico de las cintas (traídas el CR) y registra dicho estado en el documento ¸ en la solapa correspondiente al mes de realización del resguardo mensual, debe realizar también el control de los **Id** de las cintas y el tipo, corroborando que las mismas coincidan con lo registrado en la planilla antes mencionada. Si existen discrepancias debe solucionarlas. También debe ingresar la fecha de realización del backup

mensual y actualizar la columna de **Reutilización Nº**. Luego de chequear estos datos y de actualizar el documento, el Operador de Resguardo coloca las cintas en las correspondientes unidades de resguardo de los equipos.

9. El Operador de Resguardo, una vez finalizada la tarea de resguardo mensual, debe actualizar el documento ubicando la solapa correspondiente al mes en curso para completar la columna denominada **Status del Log.** Si el estado de registro del log de alguna cinta, llegase a ser “Cambiar Cinta”, debe proceder como indica el punto 6.3.3 y proceder a realizar un nuevo resguardo de dicho equipo.

6. Autorización del personal

La generación, actualización y publicación de las listas de personal autorizado para acceder al CR se describe en PE-SEG-T-nn-Autorización Traslado Medios y Acceso Sitios (Medios: dispositivos de almacenamiento).

Dependencia del TDC

El TDC del ORGANISMO, depende del Director de la DNSAFD (Director Nacional de Sistemas de Administración y Firma Digital), o la que en el futuro la reemplace.

Tiempo de guarda de la información

La información de resguardo alojada en las cintas se debe mantener por el tiempo que determina la siguiente tabla:

Tipo de información-datos	**Período de Guarda**
Código Fuentes	Perpetuo
Bases de Datos	Perpetuo

Pistas de Auditorias (logs)	3 años
Archivos de trabajos de usuarios	3 años
Lotes generados por XXXX	Perpetuo

G. Registros:

Identificación	Responsable	Archivo			Disposición	Acceso
		Lugar	Forma	Tiempo		
LT-TDC-T-01 Planilla Backup-Cintas	TDC	Servidor/ Carpeta	Electrónica/Papel	3 años	Borrado/Destrucción	TDC
LT-TDC-02 Sistemas OP y Logs de backups	TDC	Servidor/ Carpeta	Electrónica/Papel	3 años	Borrado/Destrucción	TDC
LT-TDC-T-03 Planilla de Inventario de Cintas	TDC	Servidor	Electrónica	Permanente	Permanente	TDC
FO-TDC-T-01 Etiqueta de destrucción parcial	TDC	Carpeta	Papel	3 años	Destrucción	TDC
FO-TDC-T-03 Extracción-Guarda Medios Magnéticos	TDC	Carpeta	Papel	3 años	Destrucción	TDC

H. Naturaleza de los Cambios:

Versión	Fecha	Comentario / Motivo de modificación	Autor
0		Versión Original	N y A
1			

República Argentina - Poder Ejecutivo Nacional
2021 - Año de Homenaje al Premio Nobel de Medicina Dr. César Milstein

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2021-42475463-APN-DNCOPRCYFC#JGM

CIUDAD DE BUENOS AIRES
Jueves 13 de Mayo de 2021

Referencia: Politicas de Back Up y Restauración - ONC

El documento fue importado por el sistema GEDO con un total de 26 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2021.05.13 12:40:52 -03:00

Lisa María HAEDO
Directora Nacional
Dirección Nacional de Contrataciones de Obra Pública, Registro de Constructores y Firmas Consultoras
Jefatura de Gabinete de Ministros

Digitally signed by Gestion Documental Electronica
Date: 2021.05.13 12:40:52 -03:00