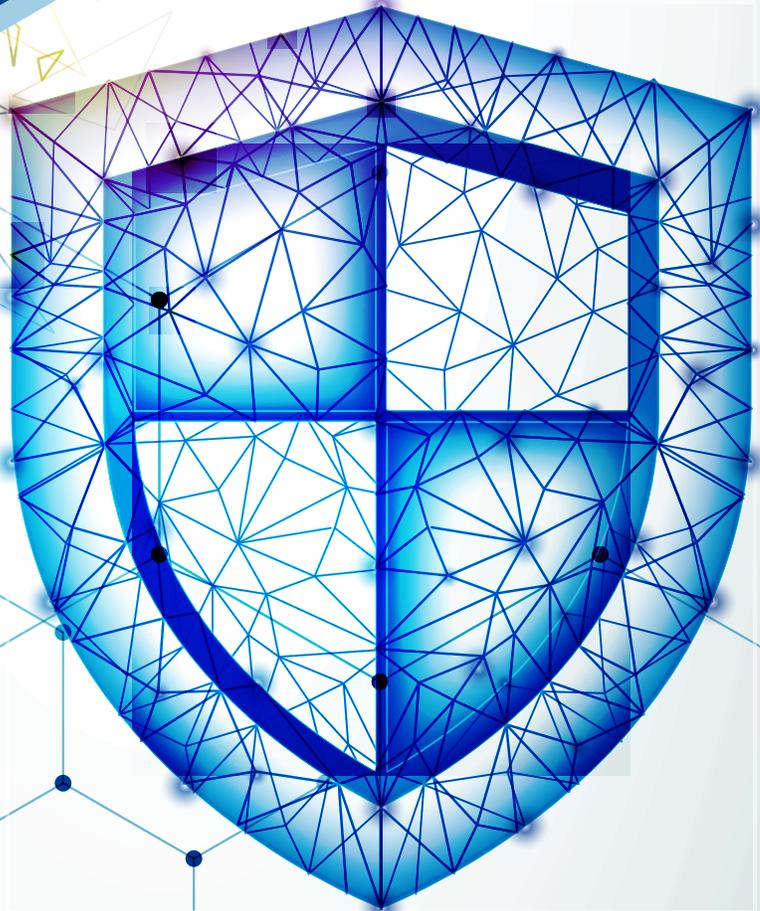


MANUAL DE RESPALDOS DE INFORMACIÓN



INTRODUCCIÓN

En la Secretaría de las Infraestructuras y el Ordenamiento Territorial Sustentable se tiene como una prioridad la protección de la información que se genera en sus diferentes áreas. Por lo que se crea el plan de respaldos de información de los equipos de cómputo y sistemas informáticos.

El Plan contiene los procesos que se llevaran a cabo para generar los respaldos y mantener la integridad de la información generada por cada una de las áreas de esta secretaria.

Este Plan de Respaldos de la Información complementa al Plan de Recuperación de Desastres Informáticos y se cumple con uno más de los objetivos del Plan de Tecnologías de la Información y Comunicación.



Objetivo.

Asegurar y mantener la integridad de la información, generada por las diferentes áreas de esta secretaria, a través de procedimientos de respaldos periódicos evitando la pérdida de información causada por una posible contingencia de desastre o eliminación accidental de la información almacenada en los equipos de cómputo y/o de los sistemas informáticos.

Objetivos específicos.

- Generar los procedimientos para la realización de los respaldos de información.
- Identificar y analizar la actividad de respaldo de información
- Documentar los procesos de respaldos e incidencias.



1.CONDICIONES PARA RESPALDOS

La realización de los respaldos será responsabilidad de los jefes de cada área, garantizando que la información institucional sea guardada en las plataformas tecnológicas destinadas para el almacenamiento de datos. Los mandos o superiores con nivel 20 o superior, de acuerdo al MANUAL DE ORGANIZACIÓN DE LA SECRETARÍA DE LAS INFRAESTRUCTURAS Y EL ORDENAMIENTO TERRITORIAL SUSTENTABLE, serán los que determinen los siguientes puntos:

1. Determinar el tipo de información que se respaldara, basado en los criterios de respaldo).
2. La periodicidad de respaldo de información conforme a los tiempos estipulados.
3. Cantidad de personas que tengan acceso al respaldo de información.

No se podrá almacenar información de índole personal en los medios destinados para el respaldo de información.



1.CONDICIONES PARA RESPALDOS

1.1 Criterios de Respaldo.

1.- Niveles de información:

Los niveles de información determinaran que características deberá tener la información para estar alojado en el almacenamiento de respaldos.

- Archivos institucionales.
- Base de datos.
- Aplicaciones con licenciamiento.

2.- Grado de respaldos:

Los respaldos se ajustarán de acuerdo al tipo de método que se requiera en cada área (completo, parcial, incremental):

Completo: Respaldo de información total de un determinado equipo o equipos, sistemas o base de datos, sin que estos se vuelvan a actualizar. E

Parcial: Respaldo parcial de información, la cual no se actualizará y tampoco aumentará.

Incremental: Información que estará en actualización constante y aumento de recursos de almacenamiento.

3.- Frecuencia de respaldos:

Los respaldos de tipo incremental son los que se actualizan constante mente y puede aumentar o disminuir su tamaño. Estos podrán realizarse de manera diaria, semanal ó mensual el cual lo determinara un mando con nivel 20 o superior.



1.CONDICIONES PARA RESPALDOS

1.2 Ubicación y resguardo de los medios de respaldo.

Garantizar la custodia de las unidades de respaldo se determina de la siguiente manera:

1.- Unidades externas: Los respaldos que se realicen en unidades externas (HDD ó SSD) serán resguardados por áreas superiores con nivel 20 o superior. Su ubicación será dentro de las instalaciones que ocupada la SINFRA y en el área que estén mejor resguardado, sin acceso a personal no autorizado.

2.- Servidores de respaldo: Los respaldos que se realicen en servidores destinados para respaldos de información deberán de estar ubicados fuera de las instalaciones que ocupada la SINFRA, siendo oficinas alternas el lugar indicado para dicho servicio. Si el servicio de respaldo se provee por parte de la DGTID (Dirección General de Tecnologías e Innovación Digital) de Oaxaca, será esta dependencia los que determinen el lugar y las reglas de almacenamiento.

1.3 Monitoreo y copias de seguridad.

El monitoreo de los dispositivos externos de respaldo se realizarán permanentemente por parte del Departamento de Soporte Técnico de la SINFRA, buscando archivos o registros que contengan virus o registros dañados. En caso de encontrar un registros o virus se procederá a un escaneo exhaustivo en búsqueda de virus y escaneo de registros dañados para corregir las fallas detectadas.

Los servidores de respaldo que se encuentren a resguardo de la DGTID, serán monitoreados por esta dirección. Siendo la DGTID quien determine los tiempos de copias de seguridad y los pasos a seguir cuando se encuentre una alarma o sospecha en la calidad de los respaldos.

Los servidores que en su momento se encuentren a resguardo de la SINFRA, serán monitoreados y administrados por el Departamento de Soporte Técnico, el cual generara los respaldos semanalmente. El servidor se localizará en oficinas alternas, con el fin de proteger al servidor de algún desastre o bloqueo de las instalaciones.



1.CONDICIONES PARA RESPALDOS

1.4 Cambios o actualizaciones de las unidades de respaldo.

Las unidades de respaldo externas se cambiarán una vez que estas unidades se encuentren llenas en su totalidad o se encuentren con registros que no se puedan reparar. Las unidades externas que se encuentren llenas quedaran a resguardo del área con un nivel 20 o superior.

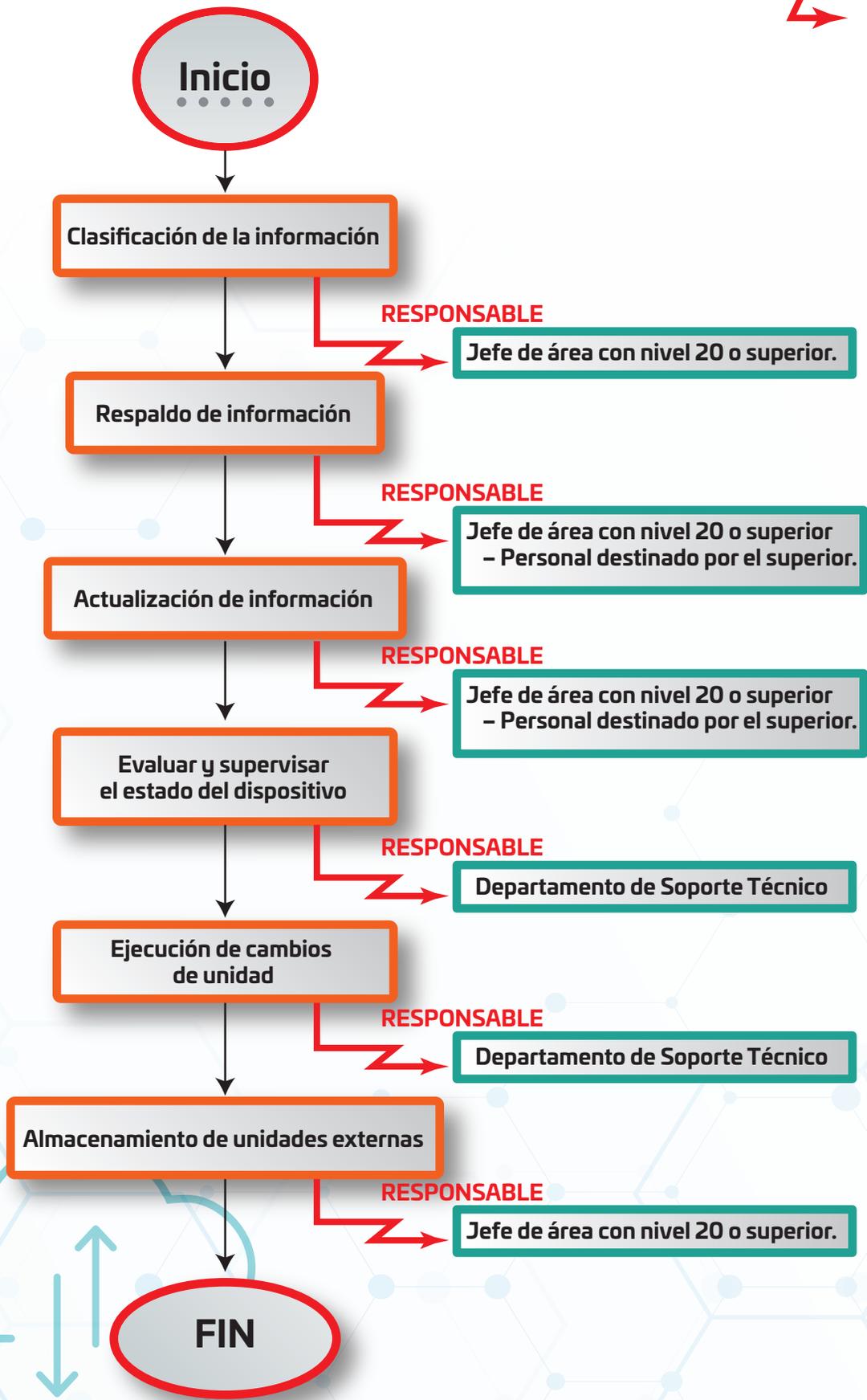
Los servidores que estén a cargo de la SINFRA se actualizarán en su firmware según lo requiera el software.

Cuando los discos duros se encuentren casi llenos de la información de los respaldos, estos se depurarán pasando la información a discos duros externos, dejando en el servidor la información de los años más recientes.



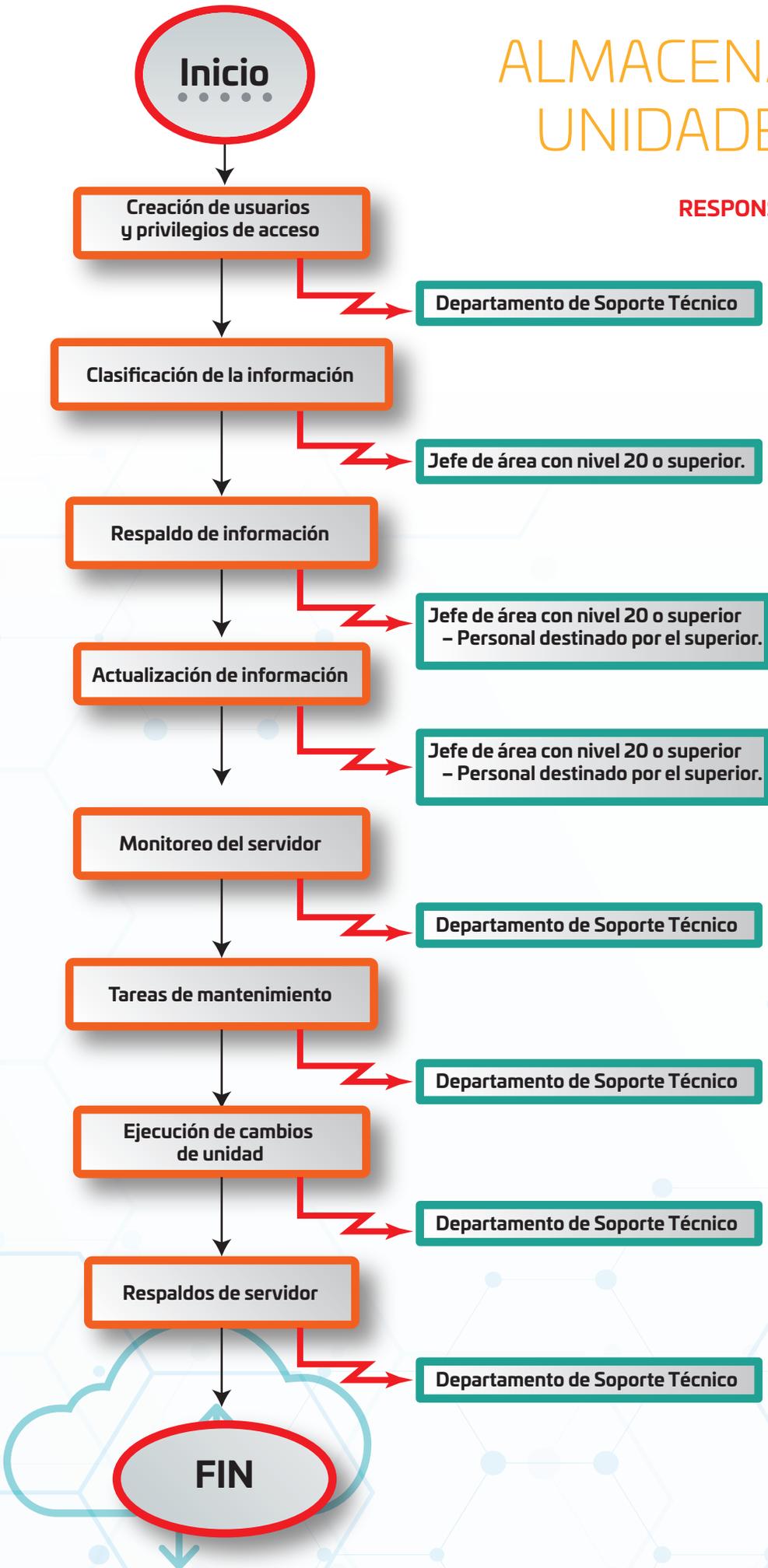
PROCESO DE RESPALDO DE UNIDADES EXTERNAS

RESPONSABLE 



ALMACENAMIENTO DE UNIDADES EXTERNAS

RESPONSABLE 



FORMATO DE INCIDENCIAS

INDICENCIAS DE SERVIDOR

FECHA DEL INCIDENTE: _____

DISPOSITIVO Y PROBLEMA

Servidor: _____ N° de Serie: _____
Discos que presentaron el problema: _____ Capacidad: _____ Gb
Problema: _____

INFORMACIÓN EN RIESGO

Tamaño de la Información: _____ Gb
Áreas que presentan el problema: _____

Usuarios que tienen Problemas: _____

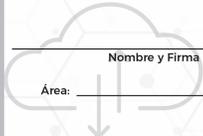
ÁREA DE ATENCIÓN

Área: _____
Atendió: _____
Capacidad de la información: _____ Gb
Capacidad Recuperada: _____ Gb
Acciones realizadas: _____

Recibe de Conformidad Vo. Bo.

Nombre y Firma Nombre y Firma

Área: _____ Área: _____



INDICENCIAS DE RESPALDOS EN DISPOSITIVOS EXTERNOS

FECHA DEL INCIDENTE: _____

REPORTE DEL PROBLEMA

Área: _____
Nombre: _____
Puesto: _____

DISPOSITIVO

Dispositivo: _____ N° de Serie: _____
Capacidad: _____ Gb
Problema: _____

ÁREA DE ATENCIÓN

Área: _____
Atendió: _____
Capacidad de la información: _____ Gb
Capacidad Recuperada: _____ Gb
Acciones realizadas: _____

Recibe de Conformidad Vo. Bo.

Nombre y Firma Nombre y Firma

Área: _____ Área: _____



INDICENCIAS DE RESPALDOS EN DISPOSITIVOS EXTERNOS

FECHA DEL INCIDENTE: _____

REPORTE DEL PROBLEMA

Área: _____

Nombre: _____

Puesto: _____

DISPOSITIVO

Dispositivo: _____ N° de Serie: _____

Capacidad: _____ Gb

Problema: _____

ÁREA DE ATENCIÓN

Área: _____

Atendió: _____

Capacidad de la información: _____ Gb

Capacidad Recuperada: _____ Gb

Acciones realizadas: _____

Recibe de Conformidad

Vo. Bo.

Nombre y Firma

Nombre y Firma

Área: _____

Área: _____



INDICENCIAS DE SERVIDOR

FECHA DEL INCIDENTE: _____

DISPOSITIVO Y PROBLEMA

Servidor: _____ N° de Serie: _____

Discos que presentaron el problema: _____ Capacidad: _____ Gb

Problema: _____

INFORMACIÓN EN RIESGO

Tamaño de la Información: _____ Gb

Áreas que presentan el problema: _____

Usuarios que tienen Problemas: _____

ÁREA DE ATENCIÓN

Área: _____

Atendió: _____

Capacidad de la información: _____ Gb

Capacidad Recuperada: _____ Gb

Acciones realizadas: _____

Recibe de Conformidad

Vo. Bo.

Nombre y Firma

Nombre y Firma

Área: _____

Área: _____

