

# CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR

ARCOTEL

**CIBERCONSEJOS  
"RESPALDO COPIAS DE  
SEGURIDAD"**

 <https://www.ecucert.gob.ec/>

 @EcuCERT\_EC

# Introducción

El desarrollo tecnológico ha permitido tener una sociedad más interconectada; generando un ecosistema en donde se distribuye una gran cantidad de información generada por Empresas, Instituciones, Academia y público en general.

Hoy en día la información es uno de los activos más preciados; sin embargo, ya sea a nivel empresarial o del común de las personas, no se realiza respaldos de información y mucho menos se verifica si el respaldo generado contiene la información requerida.

En este sentido, los diferentes actores del ecosistema digital; tienen la responsabilidad de establecer un procedimiento para hacer copias de seguridad y que permita restaurar los diferentes servicios; así mismo, se deberá controlar los soportes utilizados y vigilar que el personal autorizado sea el único que pueda acceder a estos backups.



Imagen relacionada a Información



<https://www.ecucert.gob.ec/>



@EcuCERT\_EC

01

# Criterios respaldos de información



## a) Determinar la información a copiar.

Respaldar toda la documentación de una institución sería una actividad desgastante en tiempo y en recursos; por eso es importante realizar un inventario y clasificación de activos de información.

En este inventario **se recomienda registrar tanto el software y los datos –información- que sea relevante** para la organización/institución; con esta información, se podrá determinar la periodicidad de los respaldos y el contenido de los mismos.

Entre los criterios que se pueden emplear para clasificar la información se encuentra:

- Accesibilidad.
- Utilidad.
- Impacto.
- Ciclo de vida (vida útil y vigencia del contenido).



<https://www.ecucert.gob.ec/>



@EcuCERT\_EC

02

# Criterios respaldos de información



## b) Periodicidad de copias

La frecuencia de respaldo de la documentación puede ser considerada por los siguientes factores:

- Costo de almacenamiento.
- Cumplimiento de normativa legal vigente.
- Volumen de archivos generados.



## c) Tipos de copia de seguridad

Hasta este punto se ha definido qué información debo respaldar y cada que tiempo debo ejecutar esta actividad; en esta sección se deberá elegir el tipo de copia de seguridad a implementar, entre las que se menciona:

- Copia de seguridad RAID 1.
- Copia de seguridad completa.
- Copia de seguridad incremental.
- Copia de seguridad diferencial.



# Criterios respaldos de información



- **Copia de seguridad RAID**

También conocida como “espejo”, permite realizar una copia de seguridad en tiempo real (si borramos un archivo de la sección original también se borrará de la copia); esta técnica permite una recuperación de datos de una manera ágil.

- **Copia de seguridad completa.**



Es una técnica muy empleada y consiste en copiar todos los datos del sistema en otro dispositivo; es decir, cada vez que se realicen respaldos a través de esta técnica la información se irá duplicando; provocando que existe información redundante, se necesite un mayor espacio de almacenamiento y emplear más tiempo para realización de copias de seguridad.

Por otro lado, se sugiere realizar copias de seguridad completas cada cierto periodo de tiempo acompañado de copias incrementales o diferenciales.



<https://www.ecucert.gob.ec/>



@EcuCERT\_EC

# Criterios respaldos de información



- **Copia de seguridad incremental**

Únicamente se copian los datos que han variado desde la última copia de respaldo realizada; tanto el espacio de almacenamiento como el tiempo de realización es menor en comparación con una copia completa.

- **Copia de seguridad diferencial.**



Esta técnica copiará TODOS los datos que se hayan modificado desde el respaldo anterior; es decir en su primera realización es idéntica a la copia de seguridad incremental y conforme se va desarrollando en el período de tiempo, se convertirá en una copia completa.



<https://www.ecucert.gob.ec/>



@EcuCERT\_EC

05

# Ejemplos respaldos de información



**Situación:** Información original que se desea realizar una copia de respaldo.

**Número de archivos:** 2

**Fecha:** 2022-04-22

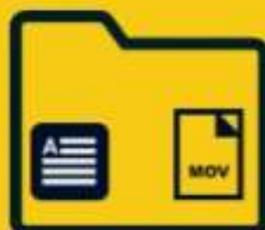
## Primera copia de respaldo

Fecha de respaldo: abril-2022

**COMPLETA**



**INCREMENTAL**



**DIFERENCIAL**



<https://www.ecucert.gob.ec/>



@EcuCERT\_EC

06

# Ejemplos respaldos de información



**Situación:** Información original que se desea realizar una copia de respaldo.

**Número de archivos:** 3

**Fecha:** 2022-05-22

## Segunda copia de respaldo

Fecha de respaldo: mayo-2022

### COMPLETA



Abril

Mayo

### INCREMENTAL



Abril

Mayo

### DIFERENCIAL



Abril

Mayo



<https://www.ecucert.gob.ec/>



@EcuCERT\_EC

07

# Ejemplos respaldos de información



**Situación:** Información original que se desea realizar una copia de respaldo.

**Número de archivos:** 4

**Fecha:** 2022-06-22

## Tercera copia de respaldo Fecha de respaldo: junio-2022

### COMPLETA



### INCREMENTAL



### DIFERENCIAL



<https://www.ecucert.gob.ec/>



@EcuCERT\_EC

08

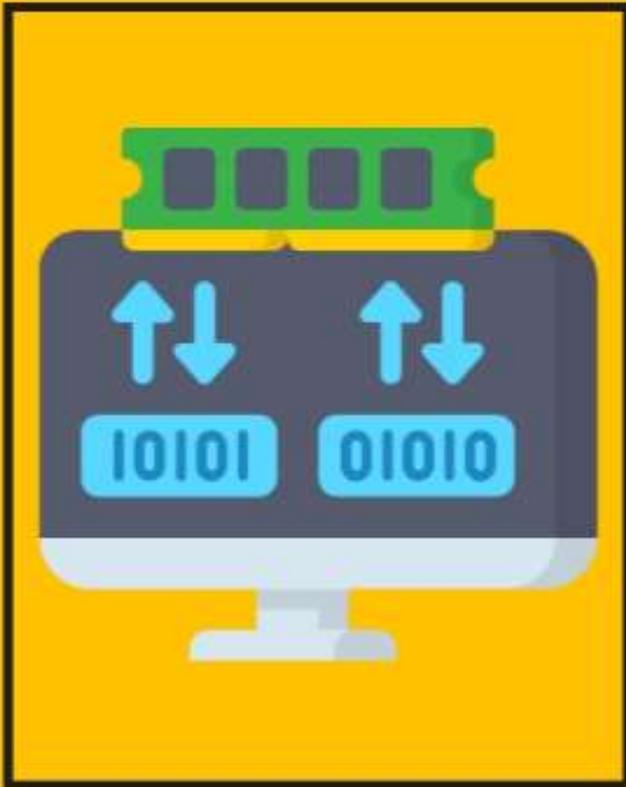
# ALMACENAMIENTO DE LOS RESPALDOS

El lugar en donde se almacenará los respaldos de información dependerá de múltiples factores; entre los que se mencionan:

- Presupuesto asignado.
- Planes de seguridad y contingencia.
- Cantidad de Información a respaldar.
- Sistema de copia seleccionado.

A continuación, se listan diferentes dispositivos de almacenamiento:

1. Cintas magnéticas.
2. Discos Duros externos.
3. Cloud.
4. Soluciones Mixtas.



# ALMACENAMIENTO DE LOS RESPALDOS

- **Cintas magnéticas.**

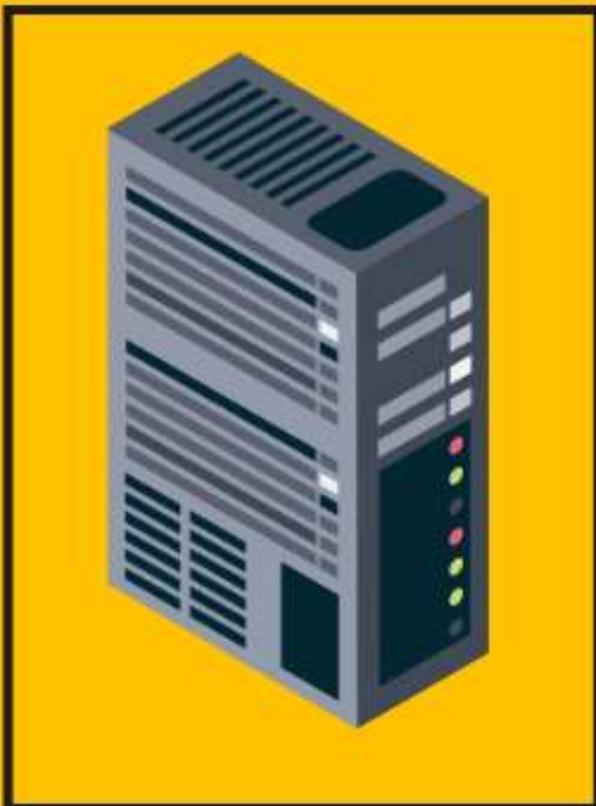
Permite almacenar grandes cantidades de datos a un reducido coste.

Según estudios; se menciona, que la vida útil de esta tecnología es de 30 años (adecuadas condiciones de temperatura, humedad, polvo, etc...)

Al emplear esta tecnología se deberá considerar librerías y accesorios adicionales para su operación; así mismo verificar la compatibilidad.

- **Discos Duros externos.**

- Presenta una mayor facilidad de configuración, mejores tasas de rendimiento, mayor capacidad de almacenamiento en comparación a las cintas magnéticas. Otra opción que se puede manejar son los **Dispositivo NAS**, que permitiría una mejor gestión de copias de seguridad.



# ALMACENAMIENTO DE LOS RESPALDOS



## • CLOUD.

La información se almacena en servidores de terceros, razón por la cual se recomienda cifrar la información a fin de evitar fugas de información y un óptimo ancho de banda de conexión a internet para un almacenamiento eficiente y una rápida descarga de la información.

## • Soluciones mixtas.

Otras soluciones que se pueden implementar es la combinación de las soluciones mencionadas anteriormente.



## Buenas Prácticas

### • Tres-Dos-Uno

Una estrategia adecuada para realizar copias de seguridad es adoptar “**3-2-1**”:

**3:** Copias de cualquier documentación o archivo importante (archivo original + 2 backups)

**2:** Almacenar las copias en dos soportes distintos.

**1:** Almacenar una copia de seguridad fuera de la infraestructura de la empresa; garantizando que la información mantenga su integridad, confidencialidad y disponibilidad.



<https://www.ecucert.gob.ec/>



@EcuCERT\_EC

# Buenas Prácticas

## • Conservación de los respaldos

Los sitios en donde se almacenan las copias de seguridad deberán brindar las garantías físicas y lógicas necesarias; así mismo, se tiene que:

- Comprobar la vida útil de los dispositivos en donde se almacena la información.
- Mantenimientos periódicos de Hardware y Software.
- Garantizar unas adecuadas condiciones ambientales del lugar en donde se almacenó la información.

## • Período de Conservación

Establecer el tiempo de almacenamiento de la información es una actividad que depende de la situación de cada institución/organización; sin embargo, se sugiere considerar estas particularidades:

- Vigencia de los respaldos y utilidad.
- Necesidad de conservar varias copias de seguridad.



<https://www.ecucert.gob.ec/>



@EcuCERT\_EC

13