Universidad Veracruzana

Buenas prácticas de seguridad para protección de la información

Ciberseguridad
UV-CSIRT

Información segura... ¡es cultura!®

Buenas prácticas de seguridad para protección de la información

Ante el incremento de ciberamenazas en las empresas y organizaciones, es importante que todos los que formamos parte de estas implementemos buenas prácticas de seguridad para proteger la información que tenemos a cargo, así como aplicarlas para la seguridad de la información personal, para ello te presentamos algunas medidas de seguridad que podrás aplicar.

1) Copias de seguridad

La pérdida de información puede presentarse de forma inesperada y provocar daños irreparables debido a diferentes causas como:

- Robo o extravío de información.
- Deterioro de los medios de almacenamiento físicos.
- Borrado accidental.
- Presencia de virus que pueden provocar la pérdida.

Por ello es fundamental realizar constantemente copias de seguridad para garantizar la continuidad de las organizaciones.

¿Cómo hacer una copia de seguridad?

Antes de realizar una copia de seguridad es importante definir cuál es la información que se debe respaldar. Para ello se debe realizar primero un inventario de activos de información y una clasificación de la misma en relación a la criticidad para la organización. De esta manera se tiene un registro de la información que sea imprescindible y así coadyuve a determinar la periodicidad y su contenido.

Periodicidad y tipos de copias

Para definir la frecuencia con la que se debe realizar una copia es preciso analizar los siguientes factores:

- Clasificación de la información de acuerdo a su importancia.
- Número de archivos creados o modificados.
- Costo de almacenamiento.
- Regulaciones legales.

Considerando lo anterior, debemos elegir el tipo de copia a realizar.

- Copias en espejo: Se crea una copia exacta de los datos en tiempo real.
- Copias de seguridad completa: Se copian todos los datos de un sistema en otro soporte.
- Copias de seguridad diferencial: Se copian todos los datos que hayan cambiado desde el respaldo anterior.
- Copia de seguridad incremental: Copia los datos que han variado desde la última copia de respaldo realizada.

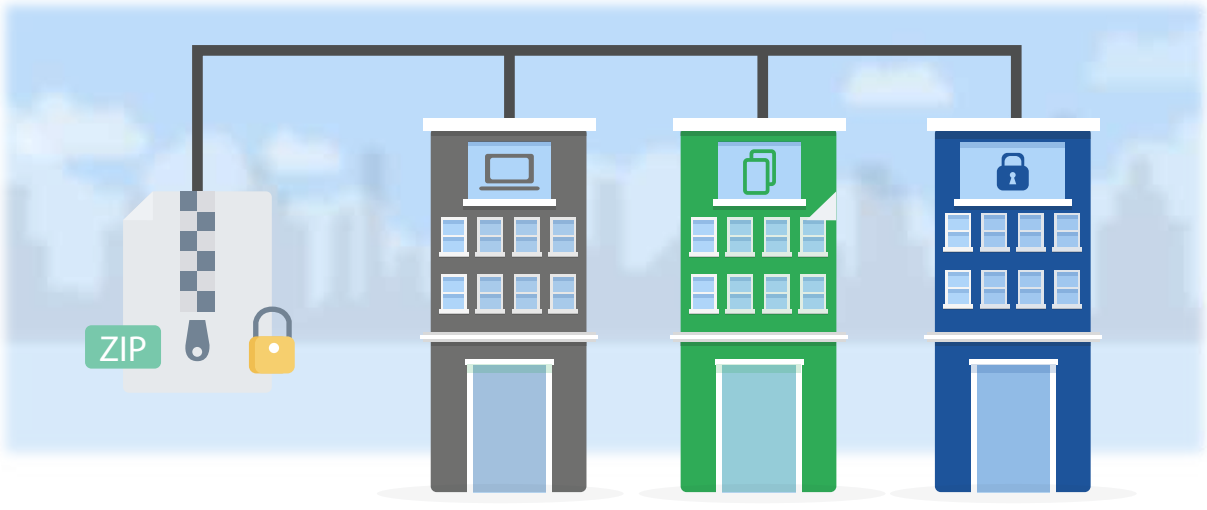
Medio de almacenamiento para realizar la copia de seguridad

El medio de almacenamiento a utilizar depende de la cantidad de información, del tipo de copia que se haya elegido y de la inversión que se quiera realizar. Estos medios pueden ser:

- Cintas magnéticas que tienen un reducido costo para almacenar gran cantidad de información.
- Discos duros.
- Nube, que permite guardar la información en servidores de terceros, en este caso es importante cifrar la información crítica que se almacene en la nube.

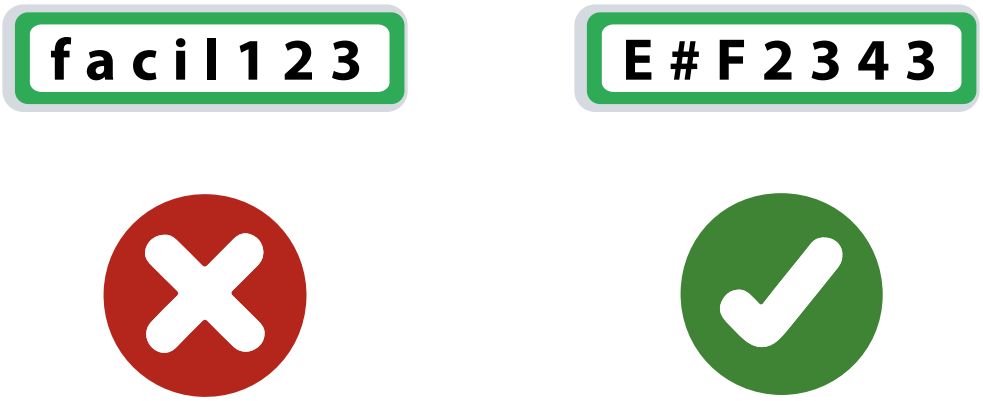
Ubicación de las copias de seguridad:

- Es importante considerar tener al menos una copia fuera de la organización.
- No utilizar un lugar personal para guardarla.



2) Cifrado de la información

Es un método en el que se convierte un texto plano en texto ilegible para que solo sea leído por la persona autorizada. Para ello, se necesita un algoritmo de cifrado y la existencia de una clave, para realizar el proceso de cifrado.



El cifrado se puede realizar en diferentes ámbitos de contenido:

- Cifrado de disco: Cifra todo el medio de almacenamiento como un disco duro o USB Esto puede llevar mucho tiempo si son varios archivos los que se cifrarán, y la velocidad de funcionamiento del disco duro se verá reducida. Algunas herramientas que se pueden utilizar son: Bitlocker, Veracrypt, Diskcryptor.
- Cifrado de carpetas: Se cifran sólo las carpetas elegidas.
- Cifrado de documentos: Cifra los archivos seleccionados. AES Crypt, cryptomator, son algunas herramientas que se pueden utilizar.

Además, es importante considerar el cifrado de la información confidencial que se decida almacenar en la nube o que se requiera compartir.

3) Borrado seguro

El borrado de la información es medida de seguridad que en ocasiones no se le da la importancia que tiene, y es que para que termine el ciclo de vida de la información, es indispensable la destrucción de la misma.

Buenas prácticas de seguridad para protección de la información

A continuación, te presentamos algunos métodos de destrucción de la información.

Métodos que no eliminan la información de forma segura

Para que se elimine eficazmente la información, es necesario que se elimine tanto la lista de archivos como el contenido del archivo. Con esto, las formas que no son métodos de destrucción de información segura son:

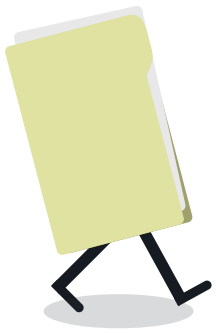
- Eliminar un archivo o carpeta con la opción eliminar o la tecla “Supr” o “Delete”.
- Formatear un dispositivo.

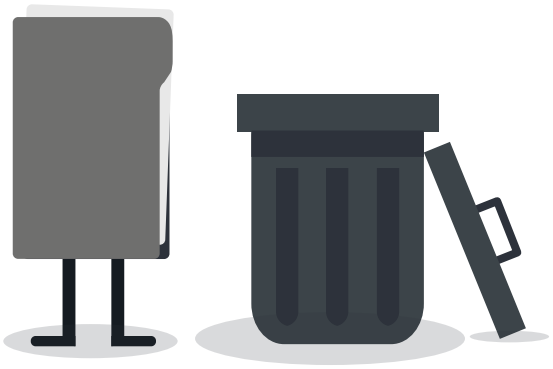
Métodos seguros para eliminar la información

- Desmagnetización.
- Destrucción física.
- Sobreescritura en la que se pueden utilizar diferentes herramientas.

Al realizar el borrado seguro evitará:

- Riesgos por robo o uso indebido de información confidencial.
- Posibles daños de imagen.
- Costos de conservación y almacenamiento.





4) Gestión de contraseñas seguras

Administrar las contraseñas de forma segura, es una de las principales medidas que las empresas deben implementar.

Buenas prácticas de seguridad para protección de la información

Para ello es importante considerar algunos puntos que NO deben realizar al usarlas.

- Crear contraseñas que sean fáciles, las que vienen por default, cortas o que se relacionen con fechas de nacimiento o datos personales.
- Escribirlas en un post-it o cualquier documento y dejarlas a la vista en tu área de trabajo.
- Compartirlas sin mecanismos de cifrado por redes sociales.
- Guardarlas en un archivo de texto.

Lo anterior, facilitaría que se presente un incidente de seguridad y con ello que exista el riesgo de una fuga de información, acceso no autorizado, alteración, borrado o pérdida de información que puede ocasionar graves daños a la organización.

Para evitar lo anterior, te compartimos los siguientes consejos:

- Generar una contraseña de mínimo 8 caracteres, usando números, letras y caracteres especiales.
- Utilizar un gestor de contraseñas, que permita cifrar todas las contraseñas en un solo archivo y recordar solo la contraseña de acceso al gestor y guardarla en un lugar seguro y generar de forma automática contraseñas aleatorias.
- Usar una contraseña distinta para cada servicio.
- Usar un segundo factor de autenticación (2FA).



Referencias:

https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_metad.pdf
https://www.osi.es/es/copias-de-seguridad-cifrado#comohacercopiasseguridad
https://cuadernosdeseguridad.com/wp-content/uploads/2020/10/recomendaciones-de-trabajo.pdf