Cómo hacer una copia de seguridad de su información personal

Definición

Una **Copia de Seguridad** es un duplicado de nuestra información personal más importante, que realizamos para salvaguardar los documentos, archivos, fotos, perfil de correo electrónico, certificados digitales, etc., de nuestro ordenador, que se realiza con el fin de poder recuperarlos en caso que se produzca su pérdida. Esta copia de seguridad también recibe el nombre de Copia de Respaldo e incluso Backup como se denomina en inglés.

Las causas que pueden provocar la pérdida de información son muy variadas, desde el mal funcionamiento de una aplicación hasta la rotura del disco duro, pasando por todo tipo de programas maliciosos como virus u otro malware. Por este motivo, resulta imprescindible planificar y llevar a cabo la planificación y realización periódica de la copia de seguridad de nuestra información personal.

Recomendaciones

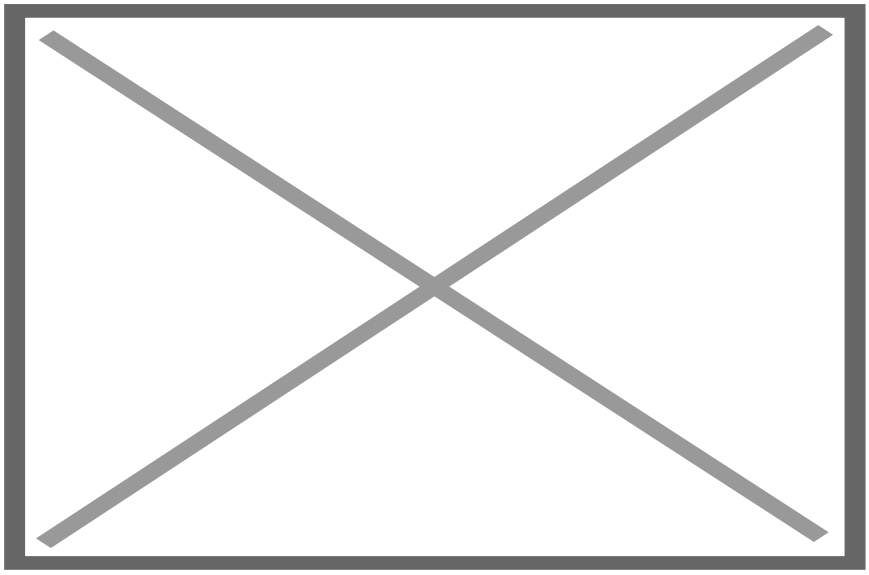
Considere el impacto que puede suponerle la pérdida de su información personal si no dispone de copia de seguridad de la misma y téngalo en cuenta la hora de seguir las siguientes recomendaciones:

- Es necesario realizar copia de seguridad de manera periódica y programada.
- Hacer la copia lo más frecuente posible, de este modo se asegurará de tener respaldo de las versiones más recientes de sus archivos personales.
- No espere a tener problemas con el equipo para llevar a cabo una copia de seguridad, puede que entonces ya sea tarde.
- Es más que recomendable disponer de copia de seguridad antes de cualquier intervención por parte del Servicio de Informática sobre su equipo (**NO esperar a realizar la copia únicamente cuando se solicite una Restauración de equipo**), cada vez que un servicio técnico manipula su equipo existe un riesgo de pérdida de información asociado.
- **Una vez realizada la copia de seguridad, DESCONECTE del equipo el dispositivo sobre el que se haya efectuado**. En caso de **Google Drive** o cualquier otro espacio en la nube (**OneDrive**, **Dropbox**, etc., no efectúe la copia sobre una carpeta que tiene sincronizada con su equipo). De otro modo, si el equipo se infecta con algún “virus” de tipo ransomware que cifre la información personal, también se cifrará la copia de seguridad haciéndola inservible.

Protocolo

Los pasos necesarios para llevar a cabo una política de copia de seguridad de forma adecuada y correcta son los siguientes:

a. **Carpeta Personal**: Es la carpeta con el nombre de usuario, comúnmente *UJA* para equipos que han sido configurados a través del SINF, que contiene todos los documentos propios de éste y otros archivos del sistema y de programas, contiene entre otras las carpetas: Escritorio, Mi música, Mis documentos, Mis imágenes, Contactos, Favoritos, Búsquedas, Descargas, Juegos guardados, etc.



b. **Certificados digitales:** Recuerde hacer copia de seguridad de su certificado digital personal (si es que no la tiene ya) que le será necesario, entre otras cosas, para la firma digital de documentos. Puede consultar el procedimiento acerca de cómo exportar e importar su certificado digital en la siguiente guía:

- Exportar el certificado digital usando Edge

- Importar el certificado digital usando Edge

c. **Favoritos y/o marcadores:** Los favoritos y/o marcadores de los navegadores deberán ser guardados también si quiere volver a recuperarlos más adelante, la ruta y método de copia varía dependiendo del navegador que se utilice, puede consultar ayuda acerca de cómo realizar la copia en los siguientes enlaces:

- Importar y exportar marcadores (Google Chrome)

1. **Hacer una lista de todo aquello que se quiere salvar**, a modo de orientación indicamos los elementos más comunes a cualquier usuario, tal y como se define en el enlace relacionado información personal:

   a. Los documentos producidos por los administradores/usuarios de los equipos con cada una de las aplicaciones que usen en su trabajo en la UJA incluyendo el sistema operativo.

   b. El perfil de correo electrónico.

   c. Los certificados digitales.

   d. Favoritos y/o marcadores de los navegadores.

   e. Cualquier otra personalización que el administrador/usuario haya hecho en el equipo desde el mismo momento que se le entregó la máquina o la adquirió por su cuenta.

   A continuación, enumeramos las **rutas y métodos de exportación de los ficheros personales y otros**

elementos antes citados necesarios a la hora de realizar una copia de seguridad:

2. **Establecer una periodicidad para la realización de la copia y tratar de cumplirla**. Para un usuario medio, una periodicidad de una semana suele ser más que suficiente. No obstante, si se encuentra realizando alguna tarea crítica, puede ser recomendable realzar copia con mayor frecuencia en base a los cambios que sufra la información relacionada con dicha tarea.
3. **Elegir el destino o ubicación de los datos de la copia de seguridad**. Existen diferentes alternativas que mencionamos a continuación. En cualquier caso, es un requisito indispensable que la copia se realice siempre fuera del propio equipo.

a. **Disco duro externo USB**. En el mercado existen distintos dispositivos externos tales como discos duros externos de gran capacidad, que pueden servir para guardar una copia de los datos fuera del disco duro del ordenador personal. **No recomendamos el uso de *Pen drivers* o *"discos llavero"* ni de tarjetas *SD* o *MicroSD,*** debido a la baja fiabilidad de este tipo de dispositivos de almacenamiento. En todo caso, es importante seguir estas pautas:

- No se puede sacar dicho dispositivo de las instalaciones de la UJA. Especialmente si tienen datos de caracter personal u otros datos sensibles.
- Se debe desconectar el dispositivo del equipo una vez realizada la copia (para evitar infecciones por ransomware).
- Se debería realizar alguna prueba de recuperación (al menos una o dos veces al año)

b. **Google Drive**. Puede utilizar el espacio de almacenamiento para cuentas de Google Workspace UJA como destino para su copia de seguridad. Recuerde que este espacio de almacenamiento es **limitado**. Este espacio se comparte entre los servicios Google Drive, GMail y fotos. Las copias manuales vía web (arrastrando y soltando los archivos), son más fiables que el cliente Google Drive para ordenadores. Recuerde no realizar la copia en una carpeta sincronizada. Tal como le indicamos con anterioridad, si el equipo se infecta con algún "virus" de tipo ransomware que cifre la información personal, también se cifrará la copia de seguridad de su espacio en la nube haciéndola inservible.

c. **Grabadora de DVDs**. Aquellos usuarios que dispongan de equipos con grabadora de DVDs puede utilizar el software de grabación Nero o cualquier otro para grabar su información personal en uno o varios DVDs.

Este método es el menos recomendado por parte del SINF debido al volumen actual de los datos de los usuarios y los altos requerimientos de espacio para la realización de la copia de seguridad.

Enlaces relacionados

- Información Personal