

# **UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA**



## **FACULTAD DE INGENIERÍA, ARQUITECTURA Y DISEÑO**

Recomendaciones para el respaldo de información y medidas de seguridad para protección de información

ENSENADA, B.C. OCTUBRE, 2024



<b>DESCRIPCION DEL EXPEDIENTE</b>		
<b>Revisión</b>	<b>Descripción del cambio</b>	<b>Fecha</b>
1.0	Elaboración del documento	30 – Oct – 2024

El presente documento tiene el propósito emitir de forma sencilla, objetiva y ordenada, recomendaciones para realizar el respaldo información, así como la implementar medidas de seguridad de la información para el personal de la FIAD.

## **I. OBJETIVO:**

Establecer las recomendaciones para respaldar/resguardar y proteger información del personal de la FIAD.

## **II. MARCO JURÍDICO:**

Manual de Procedimientos y Operaciones

## **III. DEFINICIONES**

FIAD: Facultad de Ingeniería, Arquitectura y Diseño.


USB: Universal Serial Bus.

CD: Compact Disc.

## **IV. RESPONSABILIDADES**

### **Usuarios:**

- Efectuar el respaldo de la información.
- Definir el medio y periodicidad del respaldo de información.
- Realizar el inicio de sesión.
- Utilizar contraseñas seguras.
- Efectuar acciones o medidas para proteger la seguridad de sus datos.

	<b>UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA</b> <b>FACULTAD DE INGENIERÍA, ARQUITECTURA Y DISEÑO</b>	<b>Fecha de elaboración:</b> Día <b>30</b> Mes <b>Oct</b> Año <b>2024</b> <b>Página:</b> Página <b>3</b> de <b>6</b>
	<b>DESCRIPCION DEL EXPEDIENTE</b>	
<b>Revisión</b>	<b>Descripción del cambio</b>	<b>Fecha</b>
1.0	Elaboración del documento	30 – Oct – 2024

## V. RECOMENDACIONES

### Respaldo de Información:

Un *respaldo* es una copia de seguridad que se hace de los archivos de una computadora con el fin de salvaguardarlos, poder usarlos, y evitar que se pierdan en caso de falla del disco duro.

Te recomendamos utilizar alguna de las siguientes formar para respaldar tu información.

#### 1) En un dispositivo externo

Podemos utilizar un USB, CD, disco duro externo o cintas de almacenamiento para transferir la información que consideramos es de suma importancia o relevante y deseamos evitar que se pierda, en caso de que el disco duro de nuestra computadora sufra algún daño. La cantidad de información que puedas respaldar dependerá de la capacidad del dispositivo.



Se sugiere resguardar el dispositivo en un lugar seguro para evitar pérdida del dispositivo y a su vez, perdida de la información.

#### 2) En la nube


Podemos utilizar el servicio de Google Drive asociado a nuestras cuentas de correo institucional para generar un respaldo de la información de manera gratuita y constante, dado que, podemos activar que los archivos que se respaldan estén sincronizados con nuestra computadora por lo que se actualizarán de manera simultánea o se borrarán. Recuerda que tu cuenta de Google Drive tiene un límite de 155 GB por cuenta.

Existen otros servicios que podemos utilizar para respaldar información como: DropBox, OneDrive, pCloud, Box, entre otros, que nos permiten utilizar espacio de almacenamiento en la nube de forma gratuita.

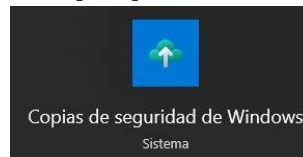


#### 3) Copia de seguridad

Tu PC Windows incluye una solución de copia de seguridad, que te ayudará a realizar copias de seguridad de muchas de las cosas que son más importantes para ti. Desde tus archivos, temas y algunas opciones de configuración hasta muchas de las

	<b>UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA</b> <b>FACULTAD DE INGENIERÍA, ARQUITECTURA Y DISEÑO</b>	<b>Fecha de elaboración:</b> Día <b>30</b> Mes <b>Oct</b> Año <b>2024</b> <b>Página:</b> Página 4 de 6
	<b>DESCRIPCION DEL EXPEDIENTE</b>	
<b>Revisión</b>	<b>Descripción del cambio</b>	<b>Fecha</b>
1.0	Elaboración del documento	30 – Oct – 2024

aplicaciones instaladas, Wi-Fi e información de cuentas que te ayudará a proteger lo que importa y que quieres respaldar [1, 2].



### **Medidas de seguridad para proteger información:**

Existen diversas medidas de seguridad que puedes aplicar para mantener segura tu información, a continuación, te damos algunas recomendaciones:


- 1) **Activar la verificación de dos factores en tu correo electrónico**, es esencial en los sistemas actuales, al utilizar tu cuenta de correo institucional se recomienda que actives esta opción para proteger el acceso a tu información [3].



- 2) **Utiliza contraseñas seguras**, estos son algunos consejos para elegir una contraseña segura de acuerdo al Instituto Nacional de Normas y Tecnología (NIST) de los Estados Unidos [4]:
  - Utilice una contraseña de por lo menos 8 caracteres.
  - No utilice contraseñas comunes ni fáciles de adivinar, ejemplo: abc123, contraseña, password, entre otros.
  - Utilice letras mayúsculas, minúsculas y números.
  - Utilizar caracteres especiales ¡ \* @ . ( \$ % ^ ) #
  - No use palabras del diccionario o nombres en ningún idioma.
  - No use nombres de equipos o el mismo nombre de la cuenta.

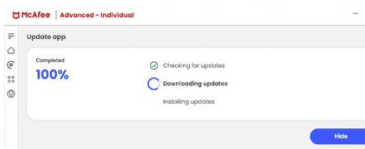
- 3) **Solo descargue software de sitios web de confianza**, para evitar la instalación de software malicioso.


- 4) **Mantenga actualizado su sistema operativo y navegador web**, instale los parches y actualizaciones de seguridad de su sistema operativo (Windows) y actualice la versión de su navegador (Chrome, Firefox, Safari, Edge, Brave, etc.).

	<b>UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA</b> <b>FACULTAD DE INGENIERÍA, ARQUITECTURA Y DISEÑO</b>	<b>Fecha de elaboración:</b> Día <b>30</b> Mes <b>Oct</b> Año <b>2024</b> <b>Página:</b> Página 5 de 6
	<b>DESCRIPCION DEL EXPEDIENTE</b>	
<b>Revisión</b>	<b>Descripción del cambio</b>	<b>Fecha</b>
1.0	Elaboración del documento	30 – Oct – 2024

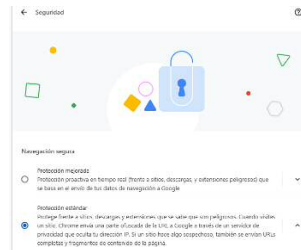


- 5) **Instale y mantenga actualizado el antivirus de su computadora**, esto le ayudará a proteger su computadora de software malicioso.



- 6) **Mantener el Bluetooth desactivado** cuando no lo esté utilizando. Dado que este protocolo se encuentra en muchos teléfonos, tabletas, mouse, teclados, etc., también puede ser vulnerado. 


- 7) **Configure la seguridad en nivel medio o alto**, establezca la configuración de seguridad en su computadora o navegador a un nivel medio o alto para proteger su equipo y datos.



- 8) **Habilite la contraseña en su equipo**, establezca una contraseña para iniciar sesión en su computadora, laptop, tableta o teléfono para evitar el acceso no autorizado.





- 9) **Cifrar datos**, el sistema de encriptación de archivos (EFS, Encrypting File System) es una característica de Windows que permite encriptar datos. Está directamente vinculado a una cuenta de usuario específica y solo el usuario que encripta los datos podrá acceder a él después de haber sido encriptados usando EFS.

	<b>UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA</b> <b>FACULTAD DE INGENIERÍA, ARQUITECTURA Y DISEÑO</b>	<b>Fecha de elaboración:</b> Día <b>30</b> Mes <b>Oct</b> Año <b>2024</b> <b>Página:</b> Página <b>6</b> de <b>6</b>
	<b>DESCRIPCION DEL EXPEDIENTE</b>	
<b>Revisión</b>	<b>Descripción del cambio</b>	<b>Fecha</b>
1.0	Elaboración del documento	30 – Oct – 2024



- 10) **Comprenda los términos sobre el uso del servicio**, revise los términos de servicio que incluyen los derechos y responsabilidades, política de uso de datos, política de seguridad, privacidad, etc.
- 11) **Acceda a información de correos seguros**, no se debe engañar, revise que su correo proviene de una fuente segura y confiable.
- 12) **Utilice la navegación privada**, cada navegador web tiene una opción para navegación privada (InPrivate, Incognito, Navegación privada, Pestaña o ventana privada) que le permitirán desactivar las cookies, archivos temporales e historial de navegación (se borrarán al cerrar la ventana o programa) para evitar la recopilación de sus datos.

 Nueva ventana de incógnito      Ctrl + Mayús + N

 Nueva ventana de InPrivate      Ctrl+Mayús+N

## VI. REFERENCIAS

[1] “Hacer una copia de seguridad de tu PC Windows - Soporte técnico de Microsoft”. Microsoft Support. [En línea]. Disponible: <https://support.microsoft.com/es-es/windows/hacer-una-copia-de-seguridad-de-tu-pc-windows-87a81f8a-78fa-456e-b521-ac0560e32338>

[2] “Respaldo y restauración de Window 10: Una guía completa”. Dell Technologies. [En línea]. Disponible: <https://www.dell.com/support/kbdoc/es-mx/000193501/c%3%B3mo-respalda-y-restaurar-en-windows-10>

[3] “Buenas Prácticas de Seguridad”. UABCiber Segura. [En línea]. Disponible: <https://cibersegura.uabc.mx/web/segura/manuales>

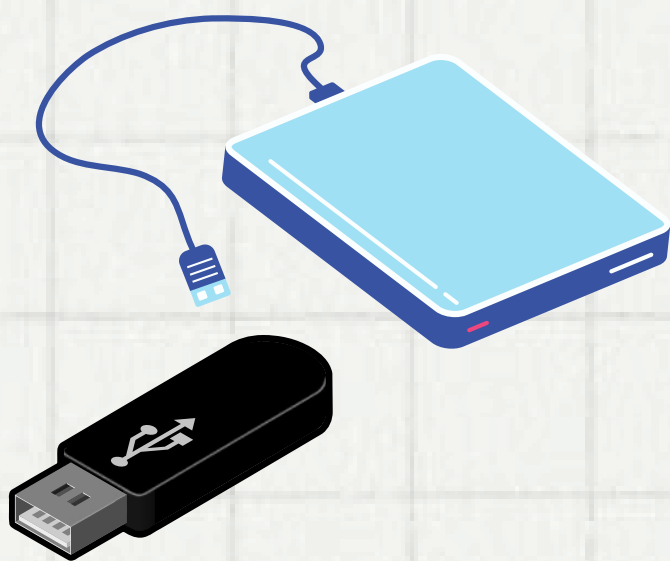
[4] “NIST SP 800-63 Digital Identity Guidelines”. National Institute of Standards and Technology. [En línea]. Disponible: <https://pages.nist.gov/800-63-3>



# 3 Formas de respaldar tu información

## Dispositivo

Utiliza un dispositivo externo como un USB, CD, DVD, disco duro externo o cinta magnética para respaldar tu información.

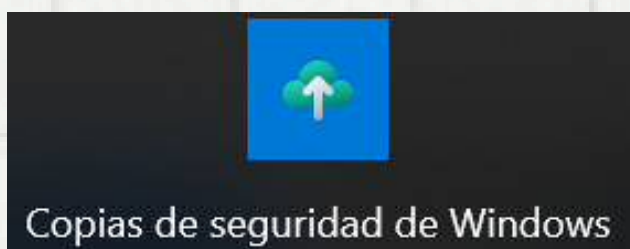


## En la nube

Utiliza Google Drive, Dropbox, OneDrive u otro servicio en la nube para tu respaldo.

## Copia de seguridad

Tu PC Windows incluye una solución de copia de seguridad, que te ayudará a realizar copias de seguridad de muchas de las cosas que son más importantes para ti.



Copias de seguridad de Windows



# Medidas de seguridad para proteger tu información

Usa verificación en dos pasos, contraseñas fuertes y seguras.



Sólo descarga software de sitios o páginas confiables.

Actualiza tu sistema operativo, programas, navegador y antivirus.



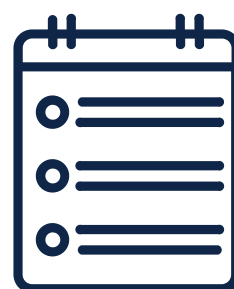
Habilita contraseña de usuario en tu equipo o dispositivo.

Sólo accede a información de correos seguros.



Mantén el Bluetooth desactivado.

Lee y comprende los términos y condiciones antes de aceptarlos.



Utiliza la navegación segura.