



Manual de Cifrado de Dispositivos

La Libre

Sobre este manual

El cifrado de dispositivos es una medida de seguridad fundamental en la era digital en la que vivimos. Consiste en proteger de datos almacenados en un dispositivo de tal manera que solo el usuario autorizado tenga acceso a ellos.

La importancia de cifrar tus dispositivos radica en la protección de información personal y confidencial. En la actualidad, almacenamos gran cantidad de información en nuestros dispositivos, como contraseñas, documentos importantes, fotografías personales, entre otros, por lo que es crucial garantizar que esta información no caiga en manos equivocadas.

Además, el cifrado de dispositivos también es importante para proteger la privacidad de las personas. En muchos casos, el acceso no autorizado a información privada puede tener consecuencias graves, como el robo de identidad o la difusión de información personal en internet. La encriptación de datos puede prevenir estos problemas y evitar que información sensible caiga en manos equivocadas.

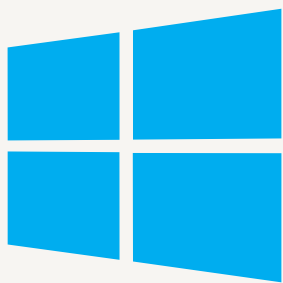
Finalmente, es importante destacar que el cifrado de dispositivos no solo protege al usuario individual, sino que también ayuda a proteger la integridad y seguridad de empresas y organizaciones. Los dispositivos móviles que utilizan los empleados en una empresa a menudo contienen información valiosa y confidencial que puede ser comprometida en caso de pérdida o robo.

El cifrado de dispositivos puede garantizar que esta información esté protegida y minimizar el riesgo de un robo de información que pueda perjudicar a la empresa y a sus clientes.





**Este manual explica como
implementar el cifrado en
dispositivos nativo con
Windows, iOS y Android
con instrucciones
especificas para cada caso**

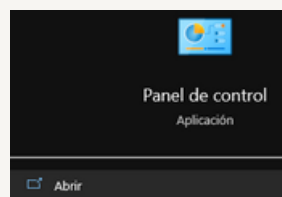
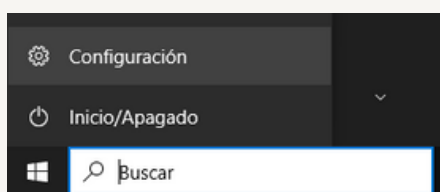


Equipos con Windows

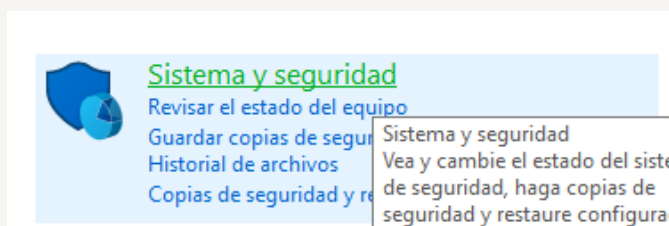
Hay que tener en cuenta que BitLocker solo funciona con la versión de Windows 10 pro y Windows 11 pro



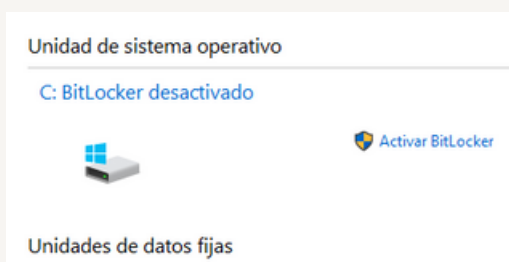
1. Nos dirigimos al buscador y ponemos **Panel de control** → y hacemos clic



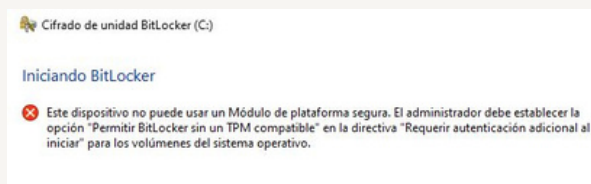
2. Ingresamos a **Sistema y seguridad** → **Cifrado de unidad BitLocker**



3. Damos clic a **Activar BitLocker**



Nota: si sale el siguiente error al activar BitLocker hay que seguir los siguientes pasos: [Corregir problema al activar BitLocker](#)



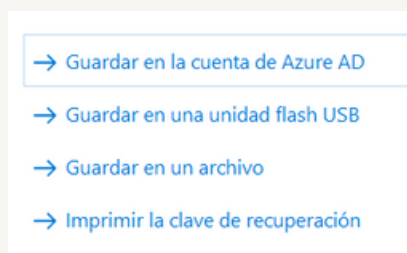
Equipos con Windows



4. Aparecen 2 opciones de como desbloquear la unidad que va a cifrar (recomendación: escribir una contraseña)



5. Escogemos la forma en la cual guardaremos la clave y la dirección donde se guardará la misma (recomendación guardarla en un archivo en una unidad externa).



6. Seguir los pasos que indica a continuación y dependiendo del espacio usado del disco duro va a demorar unas horas.

Equipos móviles

Android



Los dispositivos con Android ya vienen con la función de cifrado activa por defecto, pero para usarla hay que ponerle un pin de seguridad para

desbloquear la pantalla. Con esto aseguramos que la información del dispositivo esté cifrada mientras se encuentre bloqueado

Recomendación: usar pin o contraseña como método para bloquear la pantalla. De las opciones como huella, patrón o reconocimiento facial el pin es la más segura de todas.



Pasos para cifrar una tarjeta de memoria externa



Conecta la tarjeta de memoria externa a tu dispositivo Android.
Abre la aplicación "Configuración" en tu dispositivo Android.

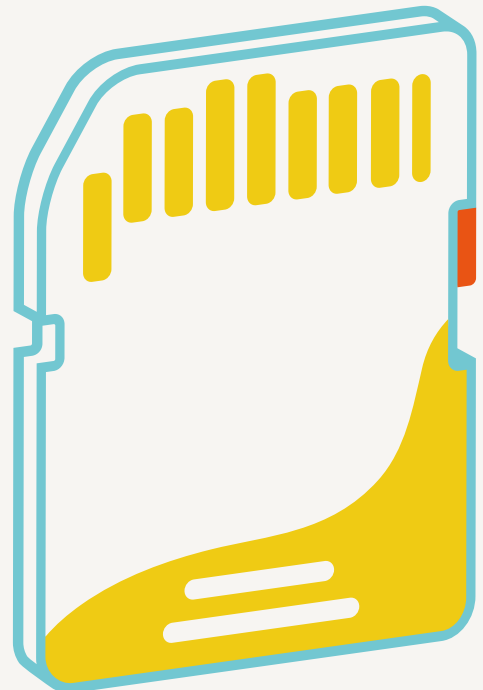
Desplázate hacia abajo y selecciona "Seguridad" o "Seguridad y ubicación" dependiendo de la versión de Android que tengas.

En la sección "Cifrado", selecciona "Cifrado de tarjeta SD" o "Cifrado de almacenamiento".

Si aún no tienes un PIN o patrón de desbloqueo establecido, se te pedirá que lo hagas. Configura un PIN o patrón de desbloqueo seguro. Selecciona "Cifrar tarjeta SD" o "Cifrar almacenamiento".

Es posible que se te pida que conectes tu dispositivo a una fuente de alimentación y esperes a que se complete el cifrado. El tiempo que tarda en completarse dependerá del tamaño de la tarjeta y de la velocidad del dispositivo.

Una vez que se complete el cifrado, podrás utilizar la tarjeta de memoria externa como de costumbre, pero ahora estará protegida por cifrado y solo podrás acceder a ella después de desbloquear el dispositivo con el PIN o patrón de desbloqueo que estableciste en el paso 5.



Equipos móviles

ios



Los dispositivos con iOS ya vienen con la función de cifrado activa por defecto. Para usarla hay que ponerle un pin de seguridad para desbloquear la pantalla.

Con esto aseguramos que la información del dispositivo esté cifrada mientras se encuentre bloqueado.

Recomendación: usar pin como método para bloquear la pantalla. De las opciones como huella, patrón o reconocimiento facial el pin es la más segura de todas.

