Syri Microsoft BitLocker





BitLocker es una característica de seguridad para el cifrado de información en cualquier unidad de nuestro equipo, la herramienta ayuda a impedir el acceso de terceros en caso de que se produzca el robo o pérdida del mismo, requiriendo que ingresemos una contraseña que hemos configurado al momento de activar la funcionalidad.

Esta guía de uso está orientada para *Windows 10 Pro/Education*, aunque también está presente en Windows 7 Pro y en sistemas Linux o Mac con herramientas de terceros.



Después, seleccionamos opción para asignar una contraseña. Continuamos en "Siguiente".







Una vez asignada la contraseña, podremos generar un archivo que contendrá la clave de recuperación (en caso de olvidarse la principal).

Sugerencia, este archivo se recomienda que sea almacenado en un lugar seguro y no sea de fácil acceso.

12	Reference de unidad BitLocker (E:)
	¿Cómo desea realizar la copia de seguridad de la clave de recuperación?
	 El administrador del sistema administra ciertas configuraciones.
	Si olvida la contraseña o pierde la tarjeta inteligente, puede usar la clave de recuperación para acceder a la unidad.
	→ Guardar en un archivo
	→ Imprimir la clave de recuperación
	¿Cómo puedo encontrar después mi clave de recuperación?

Seguridad de la informacion (E:)

	Seguridad de la informa	acion (E:)										
-	14,3 GB disponibles de	14,4 GB										
	Ruardar clave de recuperación de BitLocker como							×				
÷	- < -> < ^	→ Este equip	o > Documentos >	р			√ Ō	Buscar en p		Q		
	Organizar 🔻 N	ueva carpeta						[0		
	 OneDrive - ICE Este equipo Descargas 	SI Nor	nbre ^		Fecha de modifica 30/08/2019 11:11 a	Tipo Carpeta de archivos	Tamaño					
	 Documentos Escritorio Imágenes Música Objetos 3D Vídeos Sistema (Ci) 							Luego nos donde que el a		mostrará la ruta en eremos almacenar archivo .txt		
	Datos (D:)	la i										
	Nombre:	Nombre: Clave de recuperación de BitLocker E111E32A-2641-4875-9FA5-termente a service								~		
	Tipo: Archivos de texto (".txt) Ocultar carpetas						Guardar	Cancelar				





Una vez almacenado el archivo, continuamos presionando "Siguiente".



Nota: No olvide la contraseña digitada o el archivo de recuperación. Si los pierde, también pierde acceso a la información para siempre.

... procedemos a elegir la primera opción y damos "*Siguiente*":









Siguiente

Cancelar

iridad de la informacion (E:)

Se recomienda elegir la segunda opción para obtener una mejora compatible con respecto a versiones anteriores de Windows.

El	ección del modo de cifrado que se usará
El	ección del modo de cifrado que se usará
La Es W	a actualización de Windows 10 (versión 1511) introduce un nuevo modo de cifrado de disco (XTS-AES). te modo ofrece soporte de integridad adicional, pero no es compatible con las versiones anteriores de findows.
Si	se trata de una unidad extraíble que usarás con una versión anterior de Windows, elige el modo ompatible.
Si	es una unidad fija o si solo se utilizará en dispositivos con la actualización de Windows 10 (versión 1511) versiones posteriores, elige el nuevo modo de cifrado.
0) Modo de cifrado nuevo (recomendado para las unidades fijas en este dispositivo)
0) <mark>Modo Compatible (re</mark> comendado para las unidades que se puedan mover de este dispositivo)

Seguridad de la informacion (E:)	
14,3 GB disponibles de 14,4 GB	
 Cifrado de unidad BitLocker (E:) ¿Está listo para cifrar esta unidad? Podrá desbloguear esta unidad con una contraseña. 	
El cifrado puede tardar unos minutos en función del tamaño de la unidad. Los archivos no estarán protegidos hasta que se haya completado el cifrado.	De esta manera estará todo listo para iniciar el cifrado.
Iniciar cifrado Cancelar	





Seguridad de la informacion (E:) 14,3 GB disponibles de 14,4 GB



14,5 01		
	Cifrado de unidad BitLocker	×
	Se completó el cifrado de E:.	

Ahora podemos verificar que al intentar ingresar a la memoria USB o disco duro nos pedirá contraseña.

Syri Microsoft BitLock	er	UNIVERSIDAD ICESI
Unidad USB (E:) BitLocker Escriba la co [Más opcion	• (E:) ontraseña para desbloquear esta unidad. • •	La unidad ha quedado totalmente cifrada.

¿Cómo eliminar el cifrado?

El proceso de descifrado es más sencillo y rápido, para eso primero debemos descifrar el dispositivo ingresando la contraseña que se creó anteriormente.

Una vez desbloqueado el dispositivo presionamos clic derecho encima de la unidad y seleccionamos la opción **"Administrar BitLocker":**

Seguridad de la informacion (E:)	-
14,3 GB disponibles de 14,4 GB	Abrir Abrir en ventana nueva Anclar al Acceso rápido Cambiar contraseña de BitLocker
	Administrar BitLocker
	Escanear con Sophos Anti-Virus
	Conceder acceso a





Seleccione la opción "Desactivar BitLocker".

Inidades de <mark>datos extraíb</mark>	les: BitLocker To Go	Cifrado de unidad Bitl ocker X
Seguridad de la informa	cion (E:) BitLocker activado	
	1	Desactivar BitLocker
5	Copia de seguridad de la clave de recuperación	Se descifrará la unidad. Esto puede tardar bastante tiempo,
	Cambiar contraseña	pero puede seguir usando su equipo durante el proceso de
	Quitar contraseña	descirrado.
	Agregar tarjeta inteligente	
	Activar desbloqueo automático	Desactivar BitLocker Cancelar
	Desactivar BitLocker	

... de inmediato iniciará el proceso de descifrado.

Unidades de datos extraíbles: BitLocker To Go	Cifrado de unidad BitLocker
Seguridad de la informacion (E:) Descifrado de BitLocker	Descifrando Unidad E: 99.4% completado
~	
Unidades de datos extraíbles: Bitl ocker To Go	Administrar BitLocker
Seguridad de la informacion (E:) BitLocker desactivado	
Activar BitLocker	Cifrado de unidad BitLocker × Se completó el descifrado de E:.
	Cerrar

De esta manera, el dispositivo quedará con el **BitLocker** desactivado, por lo tanto no estará cifrado, es decir, que su acceso será libre.

