DGTIC UNAM
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Cifrado

Cursos en Línea

Cifrado

Desde que se tiene registro, la humanidad ha utilizado diversas técnicas para ocultar información de otras personas. En la era digital esto se logra con diferentes procesos de cifrado que ayudan a preservar la confidencialidad e integridad de los datos en los sistemas de información. A continuación, revisaremos algunos de los aspectos básicos relacionados al cifrado, así como algunas de las aplicaciones principales para el aseguramiento de la información en Windows.

Definición

El cifrado es un proceso por el cual es posible convertir datos en un formato incompresible o codificado que puede ser utilizado para la protección de la información impidiendo que personas no autorizadas puedan entender su contenido original. Además, puede ser utilizado para limitar el acceso a la información por medio de candados de bloqueo para usuarios no autorizados. Para lograr esto, existen diferentes técnicas de cifrado en las que se utilizan algoritmos matemáticos capaces de transformar la información para este fin. De manera análoga, es posible utilizar técnicas de descifrado para lograr que los datos vuelvan a su forma original o que permitan el acceso a la información para que pueda ser interpretada tal y como el emisor desea que el receptor autorizado lo reciba.

Figura 1. El cifrado es un elemento vital para la confidencialidad de la información.

El cifrado es esencial en numerosas aplicaciones y sistemas digitales, así como para las comunicaciones en línea, las transacciones financieras, el almacenamiento de datos sensibles y la protección de la privacidad. Sin cifrado, la información estaría expuesta a ser interceptada y leída por terceros no autorizados, lo que podría resultar en diferentes acciones negativas como puede

ser la pérdida de la confidencialidad, la divulgación de secretos o la manipulación de datos sensibles.

Elementos clave

El proceso de cifrado se basa, principalmente, en el uso de un algoritmo y una llave o clave. Estos son los dos elementos que permitirán tanto el cifrado como el descifrado de la información.

> Un algoritmo es una serie de pasos predeterminados que permiten realizar una tarea, resolver un problema u obtener un producto. En el caso del cifrado, se logra la transformación de un mensaje a un mensaje cifrado, o se limita el acceso a usuarios que no cuenten con la clave con la que el algoritmo fue ejecutado.

Los algoritmos de cifrado en el mundo digital son un elemento complejo que funciona por medio de la transformación de datos en código binario utilizando diferentes procesos matemáticos, por lo que su estudio está fuera de los alcances del curso. Sin embargo, es necesario reiterar que estos algoritmos utilizan una llave o contraseña como la clave que permite la transformación de la información en ambos procesos: tanto para cifrar como para descifrar. Pero, además, el uso de llaves en el cifrado es fundamental para conceder o limitar el acceso a la información de nuestro sistema. Por esta razón, es que las llaves son un elemento fundamental en los sistemas digitales.

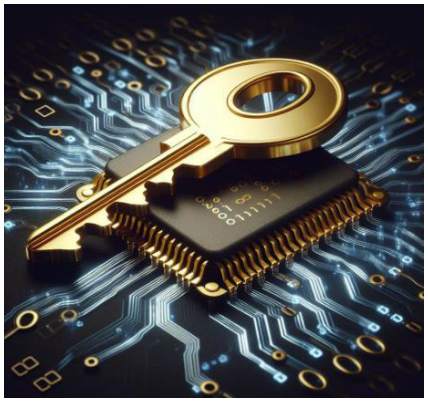

Figura 2. Las contraseñas son la llave de entrada a diferentes sistemas o archivos.

Usos en una computadora con Windows

Existen diferentes usos del cifrado en un sistema Windows. A continuación, se enlistan algunos de los más básicos que un usuario puede llegar a implementar.

Protección de archivos y folders

Windows cuenta con una característica llamada **EFS** (*Encrypting Fyle System*, en español, **Sistema de cifrado de archivos**) que nos permite cifrar el acceso a archivos o directorios en el sistema. Se puede pensar en esta característica como una caja de seguridad en la que se colocan

los archivos que deseamos proteger. El cifrado de archivos es muy útil cuando se está utilizando un sistema Windows en el que se accede de manera compartida con distintos usuarios.

> El **Sistema de cifrado de archivos** se encuentra disponible en todas las versiones de Windows excepto en las versiones Windows Home. Esto se debe a que el cifrado es un proceso que puede traer consecuencias irreversibles en el manejo de información y se considera que los usuarios de la versión profesional cuentan con un mayor nivel de destreza en el uso del sistema.

Observaremos como se puede utilizar esta función. Para comenzar, se hace clic secundario sobre el archivo o directorio que deseamos cifrar y se selecciona la opción Propiedades.

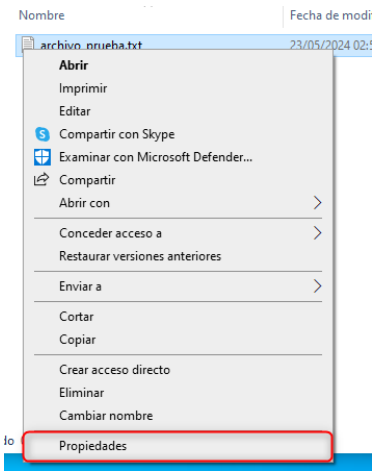

Figura 3. Menú desplegable de un archivo al hacer clic secundario con el ratón.

Se abrirá una nueva ventana con las propiedades del archivo. A continuación, se hace clic en la opción Avanzados…

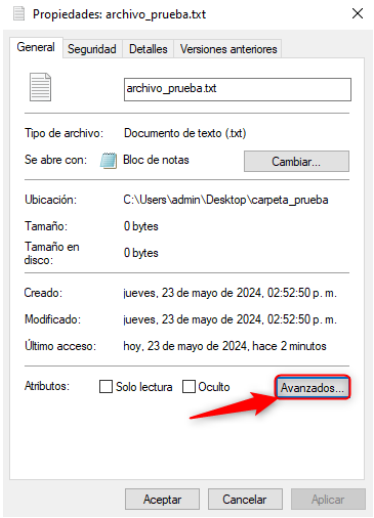

Figura 4. Ventana de propiedades de archivo.

Se abrirá la ventana Atributos avanzados desde la que marcaremos la casilla correspondiente a la opción Cifrar contenido para proteger datos. Una vez elegida la opción se hace clic en Aceptar.

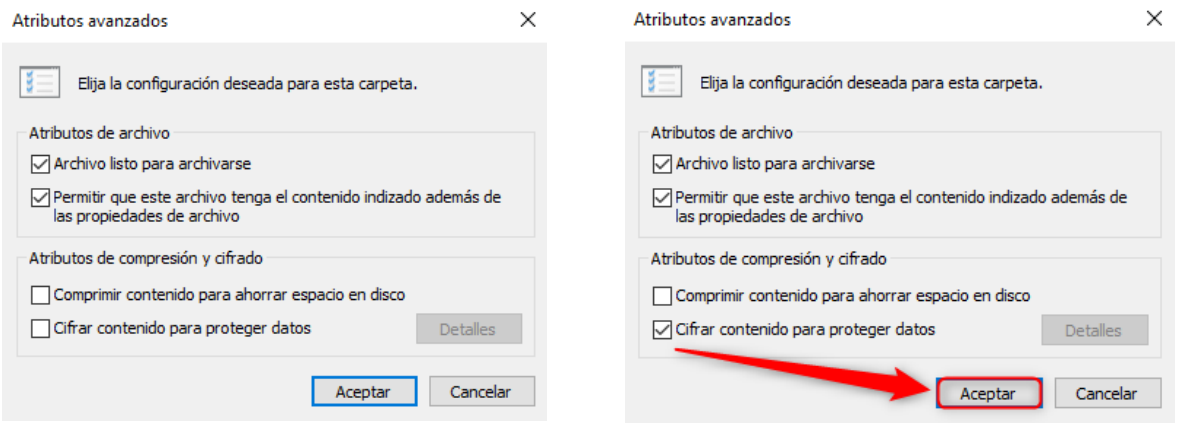

Figura 5. Activación de la casilla Cifrar contenido para proteger datos.

NOTA IMPORTANTE: Cuando se realiza el cifrado por primera vez en un equipo, aparecerá un mensaje informando que es recomendable realizar una copia del certificado de seguridad que concede el acceso al archivo. No se preocupe si no llega a hacer clic cuando aparece el mensaje ya que es posible acceder a la librería de certificados por medio del Panel de control en la sección Cuentas de usuario y en el apartado Administrar sus certificados de cifrado de archivo.

Desde la perspectiva del usuario que cifró el archivo no se apreciará ningún cambio aparente. Sin embargo, si el archivo se traslada a otra computadora, o bien, otro usuario ingresa con una cuenta distinta e intenta abrirlo, no tendrá éxito.

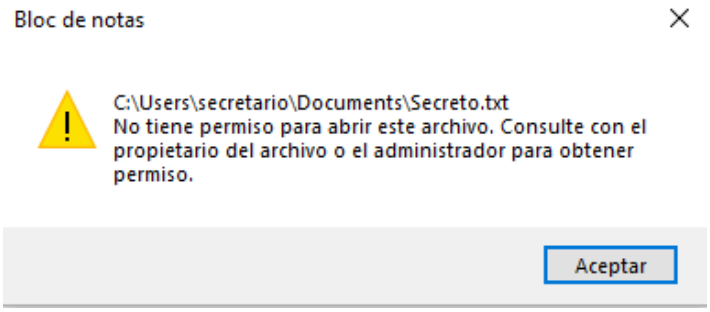

Figura 6. Mensaje de advertencia que aparece cuando otro usuario intenta acceder al archivo.

Esto sucede porque, cuando se encripta un archivo con este sistema, se liga con la cuenta de usuario de Windows con la que ha sido creada. Es importante comprender esta condición porque si alguien tiene acceso a la misma cuenta podrán ver el archivo sin problema. Por esta razón, muchos administradores señalan la necesidad de que cada usuario tenga su propia cuenta. Aun así, este tipo de cifrado es valioso para evitar que otros usuarios puedan tener acceso a nuestra información.

Se sugiere prudencia en el uso e implementación de cualquier tipo de cifrado pues, como se ha mencionado, es posible que un mal uso de las características afecte negativamente el acceso a su información. Por ejemplo, puede cifrar un archivo y al desear utilizarlo en otro equipo usted no podrá abrirlo, pues necesitaría importar el certificado de seguridad a este nuevo equipo. Sin embargo, no se recomienda importar este certificado a equipos que no le pertenezcan pues con este certificado se podrían abrir todos los archivos cifrados del equipo original.

Cifrado en MS Office

Otro de los usos principales del cifrado en un sistema Windows es aquel que se realiza en los archivos de la suite MS Office, por ejemplo, documentos de Word, Excel, PowerPoint, etc. En estos archivos es posible utilizar el cifrado para permitir el acceso solamente a aquellos usuarios que cuenten con la clave de acceso. Para esto, es posible seguir los pasos siguientes:

Desde cualquier documento de Office haga clic en la pestaña Archivo.

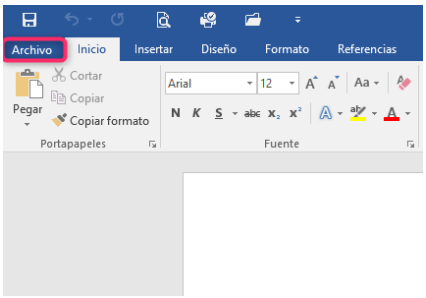

Figura 7. Ejemplo de pestaña Archivo en un documento de Word.

Posteriormente, seleccione la opción Proteger documento y seleccione del menú la opción Cifrar con contraseña.

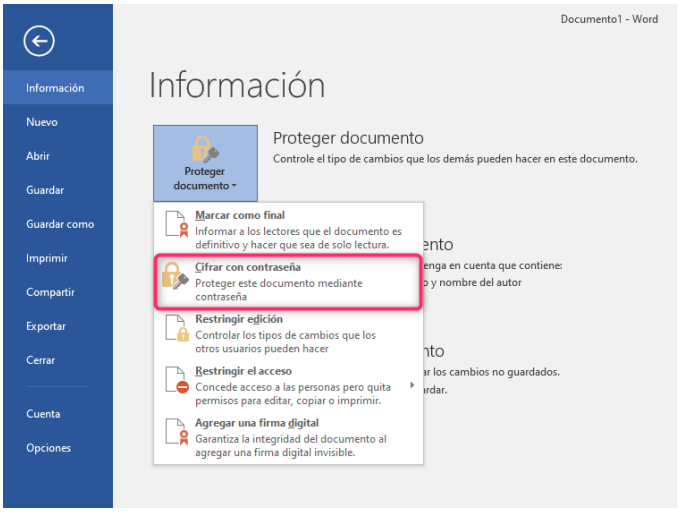

Figura 8. Vista de la opción Cifrar con contraseña.

Aparecerá un mensaje señalando que se cifrará el contenido utilizando una contraseña. Este es el espacio en el que escribirá su contraseña y en el que se le pedirá que la repita para confirmar sus valores.

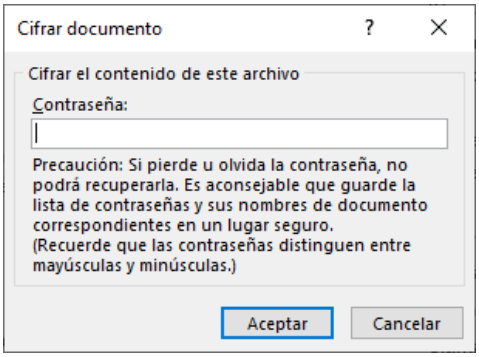

Figura 9. Vista de la ventana Cifrar documento, note los mensajes de precaución sobre la importancia de recordar la contraseña.

Una vez establecida la contraseña el documento estará cifrado y se mostrará el siguiente mensaje que indica que para abrir el documento se necesitará el ingreso de la contraseña definida.

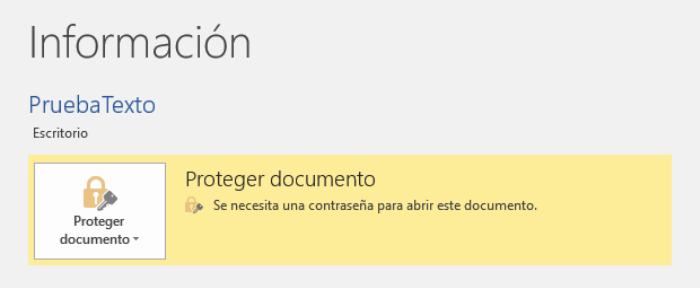

Figura 10. Documento cifrado.

Ahora, cada vez que se intente abrir el documento, se solicitará que el usuario ingrese la contraseña para poder desplegar su contenido.

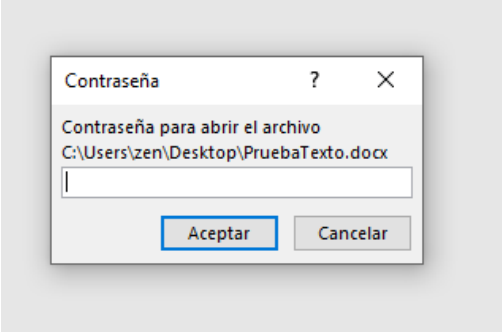

Figura 11. Ventana de solicitud de contraseña que aparecerá cada vez que el documento se intenta abrir.

El cifrado de documentos es uno de los cifrados más comunes y más fáciles de implementar con el que se puede comprobar la importancia del cifrado para la preservación de la confidencialidad de la información. Sin embargo, se hace hincapié en la necesidad de realizar los procedimientos

de cifrado de manera prudente y de experimentar con estas características en archivos que no sean muy importantes, al menos hasta que se comprenda su funcionamiento, para no comprometer su información.

BitLocker

BitLocker es una herramienta de seguridad de Windows que permite cifrar la unidad de almacenamiento principal para evitar el acceso no autorizado. Por ejemplo, en el caso de que nuestro equipo haya sido extraviado o robado, nadie podrá acceder a la información que contiene a menos que cuenten con la llave o clave de acceso.

Figura 12. BitLocker funciona como un candado de seguridad para restringir el acceso a nuestra información.

BitLocker se encuentra disponible en todas las versiones de Windows excepto en las versiones Windows Home. Esto se debe a que, al igual que se mencionó para el Sistema de cifrado de archivos, el cifrado con estas herramientas es un proceso que puede traer consecuencias irreversibles en el manejo de información y se considera que los usuarios de la versión profesional cuentan con un mayor nivel de destreza en el uso del sistema.

Al estar activado, BitLocker puede evitar el encendido normal del equipo si se detectan cambios en el sistema o no se logra comprobar la identidad del usuario. Algunos de los principales escenarios que pueden ocasionar que se active el candado de BitLocker son:

- El usuario ingresa muchas veces la contraseña incorrecta al iniciar sesión.
- Cuando se remueve el disco duro y se intenta conectar a otro equipo.
- Al cambiar el orden de dispositivo de arranque del equipo por una unidad diferente como, por ejemplo, un disco externo o la unidad CD/DVD.
- Se presentan modificaciones en los componentes de seguridad de la tarjeta madre del equipo, por ejemplo, en el chip TPM (*Trusted Module Platform*).

En cualquiera de estos escenarios BitLocker presentará una pantalla de bloqueo en la que se solicitará la contraseña creada cuando se activó la herramienta. De esta manera, evitará que cualquier persona pueda tener acceso a la información a menos que se coloque la contraseña con la que la unidad fue cifrada.

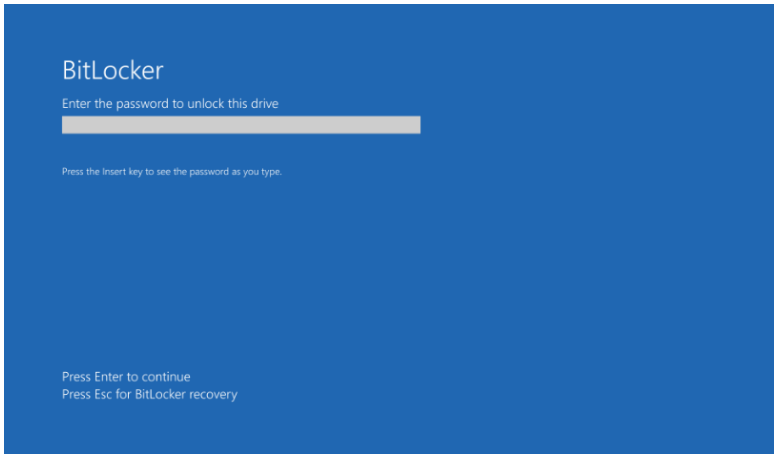

Figura 13. Ventana de bloqueo de BitLocker.

BitLocker es una opción avanzada que debe ser manejada con mucho cuidado pues el usuario puede llegar a perder el acceso a su información. Sin embargo, resulta importante conocer que existe esta opción en caso de que las necesidades de seguridad específicas de un usuario demanden su activación.

BitLocker To Go

BitLocker To Go es una modificación de la versión convencional de BitLocker que funciona para el cifrado de unidades externas como discos duros portables o unidades USB. Dada su facilidad de uso, y a que el peligro de perder información es menor, observaremos el proceso de activación.

Para comenzar, escriba en la ventana de búsqueda BitLocker y haga clic en Administrar BitLocker, o bien, desde el panel de control seleccione la opción Cifrado de unidad BitLocker.

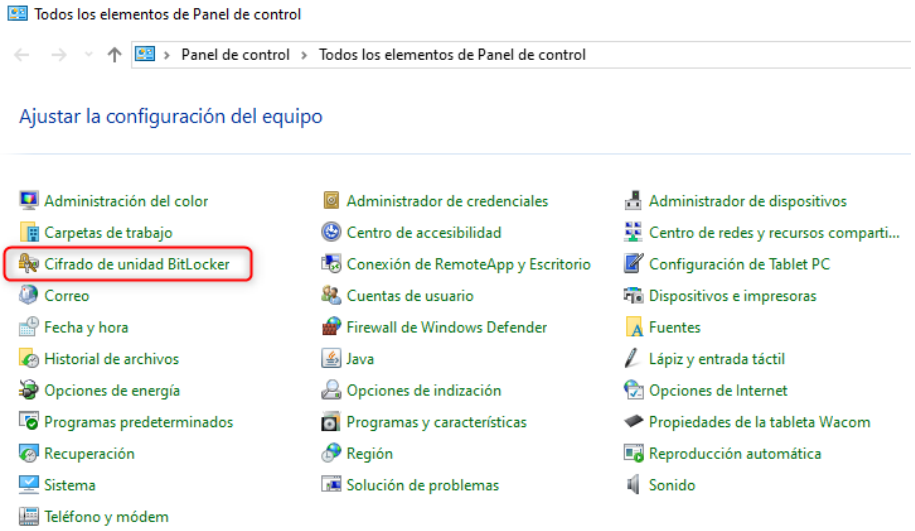

Figura 14. Vista del panel de control con la opción Cifrado de unidad Bitlocker.

Se presentará la siguiente ventana en la que se informa que es necesario insertar una unidad extraíble para usar BitLocker To Go.

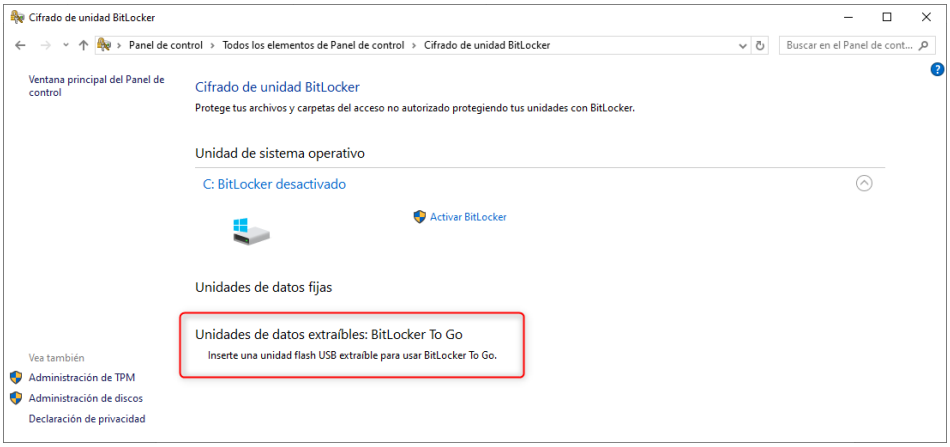

Figura 15. Recuerde que BitLocker y BitLocker To Go son herramientas distintas con usos específicos. La primera cifra la unidad de almacenamiento principal, mientras que la segunda puede cifrar unidades externas.

Al insertar una unidad extraíble, la ventana de información cambiará y reconocerá el volumen.

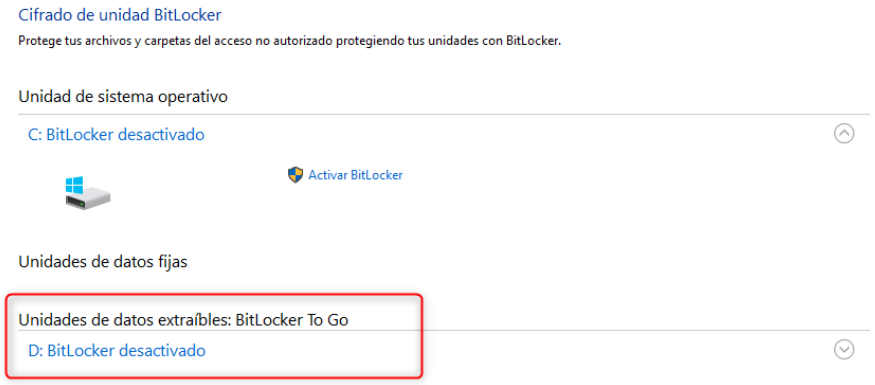

Figura 16. Imagen con la sección Unidades de datos extraíbles resaltada.

Al hacer clic sobre la unidad se presenta la opción Activar BitLocker.

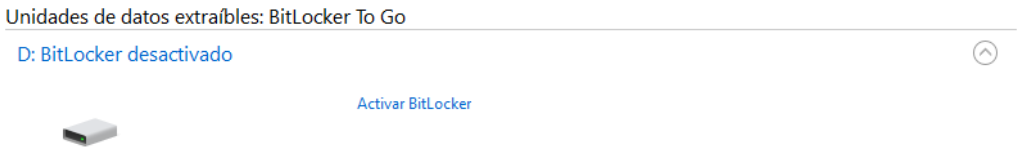

Figura 17. Vista de la opción Activar BitLocker.

Aquí se puede hacer clic en Activar BitLocker para comenzar la activación, pero recuerde que es importante hacerlo **SOBRE LA UNIDAD EXTRAÍBLE**, tenga cuidado de activar la opción de cifrado en la unidad principal. Una vez hecho el clic, comenzará el proceso de inicialización de la unidad con BitLocker, este paso puede demorar algunos minutos.

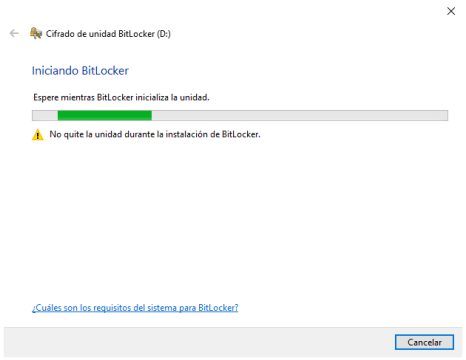

Figura 18. Ventana de inicialización de BitLocker sobre la unidad externa.

Una vez finalizado el proceso se pedirá elegir la forma en que desea desbloquear la unidad. Se sugiere utilizar una contraseña y escribirla en los campos correspondientes para después hacer clic en Siguiente.

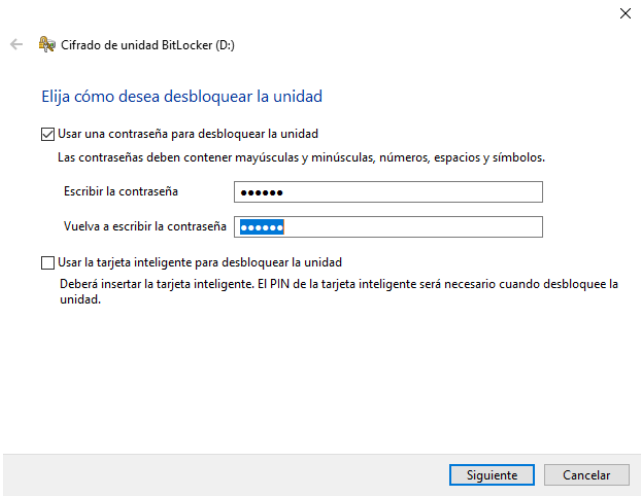

Figura 19. Ventana de selección de método de desbloqueo.

Aparecerá una nueva ventana en la que se nos informa que es recomendable guardar una copia de la clave de recuperación:

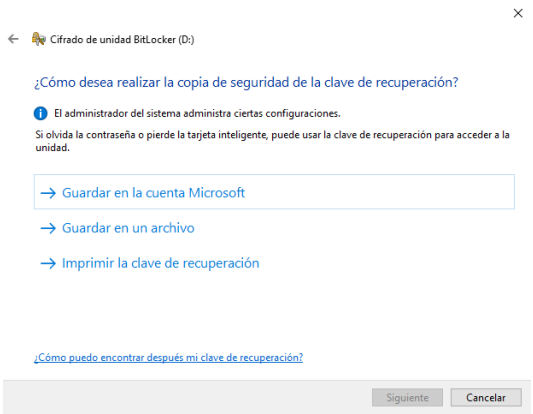

Figura 20. Ventana de selección de respaldo de clave de recuperación.

Puede seleccionar cualquiera de las opciones según sus necesidades. Por ejemplo, puede seleccionar Guardar en un archivo y elegir un directorio en su computadora donde desea que se almacene la clave de recuperación. La clave de recuperación es un archivo de texto simple similar al de la siguiente imagen:

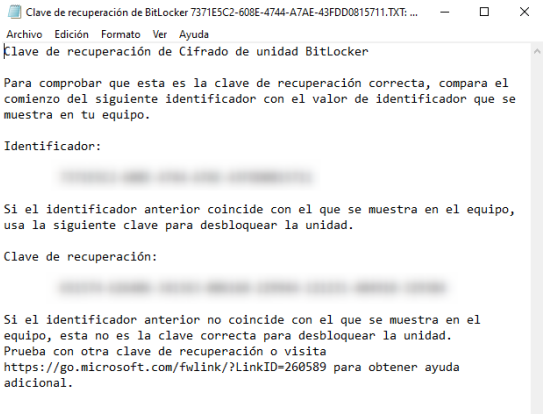

Figura 21. Imagen de un archivo de texto simple con la clave de recuperación generada.

Una vez que se ha almacenado la clave de recuperación se puede hacer clic en Siguiente. Se nos mostrará una nueva ventana en la que debemos elegir la opción correspondiente para el cifrado según nuestras necesidades y, posteriormente, seleccionamos Siguiente.

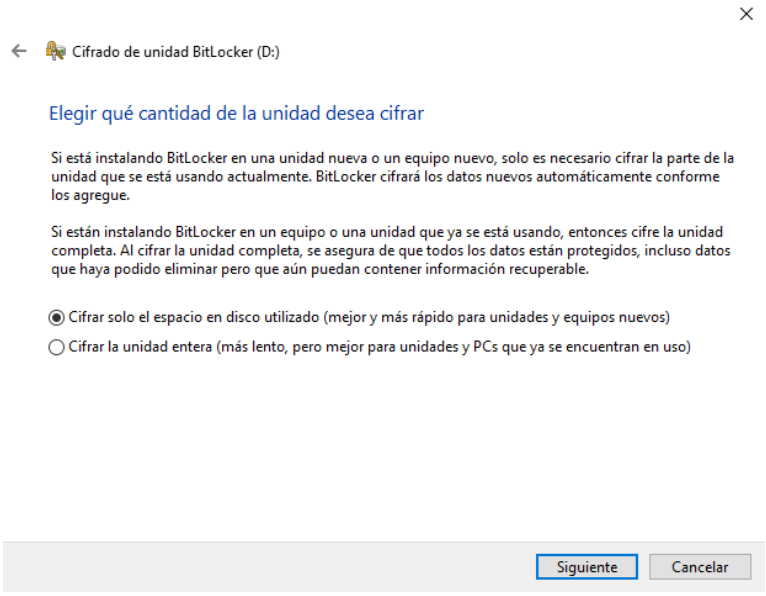

Figura 22. Selección del espacio de cifrado.

Se mostrará la siguiente ventana con opciones para seleccionar el modo de cifrado, al tratarse de una unidad USB la opción recomendable es el Modo Compatible. Se selecciona la opción y se hace clic en Siguiente.

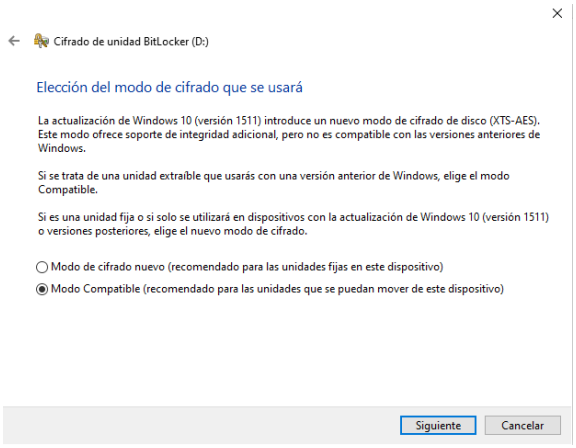

Figura 23. Selección de Modo compatible.

Aparecerá la siguiente ventana que nos informa que comenzará el cifrado al hacer clic en Iniciar cifrado.

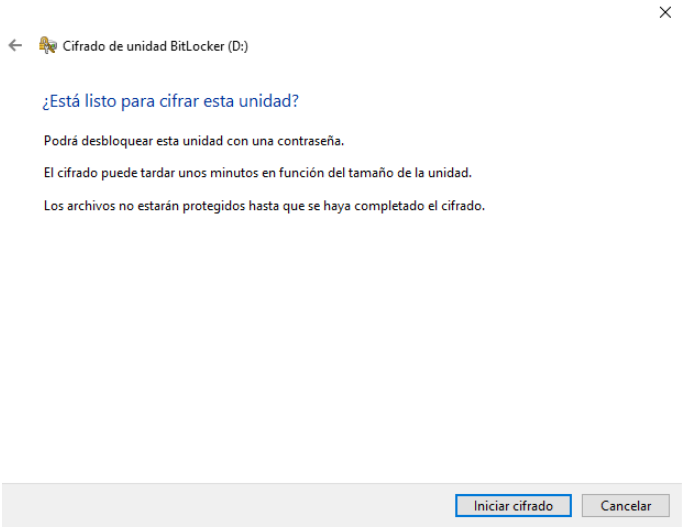

Figura 24. Ventana de inicio de cifrado de la unidad.

El cifrado comenzará y se presentará la ventana de información con el estatus de avance.

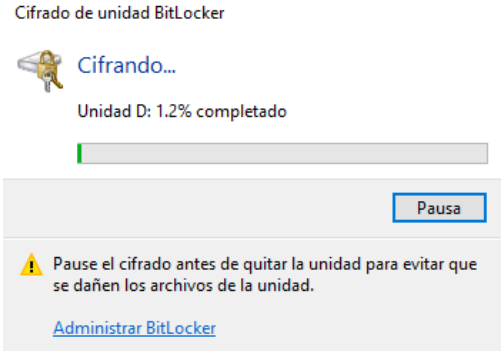

Figura 25. Estatus de avance del proceso.

Finalmente, se informará al usuario que el cifrado se completó en la unidad correspondiente.

Figura 26. Mensaje de información sobre la finalización del proceso de cifrado.

Ahora, cada vez que se inserte la unidad en algún equipo aparecerá el siguiente mensaje:

Figura 27. Mensaje de notificación de Windows al insertar una unidad externa cifrada.

Y al dar clic sobre esta notificación aparecerá la siguiente ventana donde se escribe la contraseña que se ha definido. Posteriormente, se selecciona Desbloquear y ya tendremos acceso a los archivos.

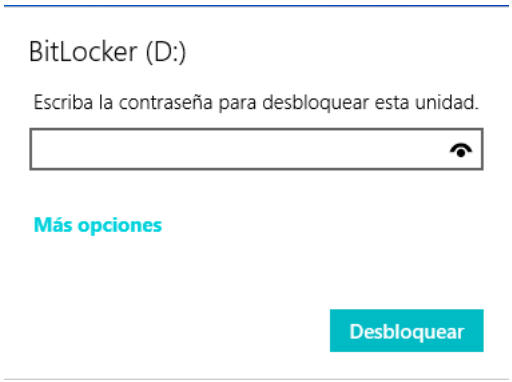

Figura 28. Ventana de desbloqueo de unidad cifrada con BitLocker.

En caso de que este procedimiento no le permita el cifrado de la unidad deberá contactar al administrador de sistemas de su organización, pues es posible que el servicio no se encuentre habilitado o que debido a las directivas del sistema no se permita su ejecución.

Como se puede observar los procesos de cifrado en Windows pueden llegar a tener un grado de dificultad considerable y tener consecuencias irreversibles para su información. Sin embargo, es importante conocer que se cuenta con estas opciones en caso de que nuestras necesidades de seguridad no los demanden

AUTOR

ELIER EMANUEL LÓPEZ BASILIO