RECOMENDACIONES PARA LA COMUNICACIÓN DE DATOS DE CARÁCTER PERSONAL Y DEL TRANSPORTE DE DOCUMENTACIÓN A TRAVÉS DE MEDIOS ELECTRÓNICOS

1. COMUNICACIÓN DE DATOS DE CARÁCTER PERSONAL

El tratamiento de los datos personales se realiza generalmente mediante aplicaciones informáticas que incorporan las adecuadas medidas de seguridad. No obstante, cada vez con mayor frecuencia existe la necesidad o la obligación de comunicar datos personales a través de cauces de comunicación electrónicos (como las aplicaciones de registro y en excepcionales ocasiones mediante el correo electrónico). En esos casos deberá valorarse la necesidad de establecer diversas medidas de seguridad, especialmente si los datos son sensibles o de categorías que requieren especial protección (como datos de salud, religión, etc.).

La comunicación de datos de carácter personal debe efectuarse de la manera más segura posible y por ello, siempre que sea posible, deberá remitirse por canales oficiales. En el caso de relaciones institucionales o laborales en las Administraciones Publicas la ley obliga a relacionarse a través de medios electrónicos, dicha comunicación se realizará **preferentemente a través de las aplicaciones corporativas accesibles a través de la intranet** y a través del **registro electrónico**, de manera que pueda quedar constancia de la tramitación.

Excepcionalmente, si no es posible remitir la información por registro, podrá emplearse el correo electrónico como forma de comunicación, aunque hay que tener en cuenta que no constituye un medio de notificación, ya que no permite asegurar la constancia fehaciente de la entrega y recepción por el destinatario.

Para remitir documentos a terceros autorizados, cuando no se disponga de un medio oficial o este no sea conveniente o adecuado, el correo electrónico debe ser la última opción y esta Delegación de Protección de Datos recomienda sustituir este canal por el uso del sistema de Nube en red. Para compartir información de carácter profesional los empleados públicos deben utilizar el sistema de registro electrónico de su organización y debe evitarse el uso de sistemas externos a la Comunidad de Madrid como, por ejemplo, Google Drive y hacer uso de Cloud, el sistema de nube corporativo de EducaMadrid, donde todos sus usuarios disponen de 5Gb de capacidad de almacenaje, ampliables a10 Gb o del Aula Virtual cuando las comunicaciones no necesiten registrarse oficialmente.

En cualquier caso, el remitente deberá tomar las precauciones necesarias para que únicamente el destinatario de la información pueda acceder a ella, dado que en el caso de cuentas de correo genéricas y unidades de registro electrónico es posible que varias personas tengan acceso a la información, para lo cual se deberán tener en cuenta las siguientes recomendaciones:

1) Los datos personales deberán incorporarse exclusivamente en uno o varios documentos anexos cifrados. No se consignarán datos personales en el campo de

asunto del correo electrónico ni en el texto del mensaje. Tampoco se harán constar en los campos de texto del asiento en el registro electrónico. Para identificar el contenido se deberán emplear datos como el número de expediente o similares. Si ello no es posible, con carácter excepcional se podrá consigna una descripción que incluya las iniciales de nombre y apellidos de la persona.

2) Se incluirá un texto explicando que la información de carácter personal se incluye cifrada, así como la identificación del destinatario final, proporcionando una dirección de correo electrónico y/o un teléfono de contacto para que dicho destinatario final pueda recabar la clave de descifrado.

Por lo tanto, y especialmente si la información contiene datos sensibles, los datos de carácter personal **nunca deben incorporarse en el texto de la comunicación**. Como se ha indicado, en lugar de ello deberá utilizarse un **documento anexo, protegido y cifrado por contraseña.** Más adelante se describe cómo proceder para cifrar un documento**.**

- La contraseña utilizada deberá cumplir los siguientes criterios:
    - Al menos **ocho** (8) caracteres
    - Para que sea suficientemente segura deberá incluir **mayúsculas** y **minúsculas**, **números** y **símbolos** o signos de puntuación.
- La **contraseña** deberá ser **comunicada** al destinatario autorizado para conocer el contenido del fichero **por medio distinto al utilizado para el envío de datos** (por ejemplo, por vía telefónica) o remitiéndola **en otro mensaje distinto**.
- Si se remite por correo electrónico, el mensaje debería incorporar la siguiente **advertencia**:

  "*Este mensaje va dirigido de manera exclusiva a su destinatario y la información contenida en él, así como la que consta en cualquiera de sus ficheros adjuntos, es RESERVADA y CONFIDENCIAL. Si Usted lee este mensaje y no es el destinatario indicado (o responsable de remitirlo a la persona indicada) por favor, comuníquenoslo por este medio y proceda a destruirlo o borrarlo. En todo caso absténgase de utilizar, reproducir, alterar, archivar, o comunicar a terceros el presente mensaje y/o ficheros anexos, pudiendo incurrir, en caso de llevar a cabo tales acciones, en responsabilidades legales.*"
- Respecto al **texto que figure en el asunto del correo electrónico o en el asiento de la entrada de registro,** deberá contener una expresión comprensible y con significado para los usuarios con acceso autorizado que les permita identificar el contenido del archivo, y **en ningún caso debe contener datos personales.**
- En cuanto a los **destinatarios a incluir en el correo electrónico** que contenga el archivo en cuestión, se deberá atender al principio de minimización de datos, de forma que únicamente se remita el correo a las personas que estrictamente resulte necesario que conozcan el contenido del mismo, de conformidad con el artículo 5 del Reglamento (UE) 2016/679 (RGPD). Igualmente, dicho principio se aplicará a la

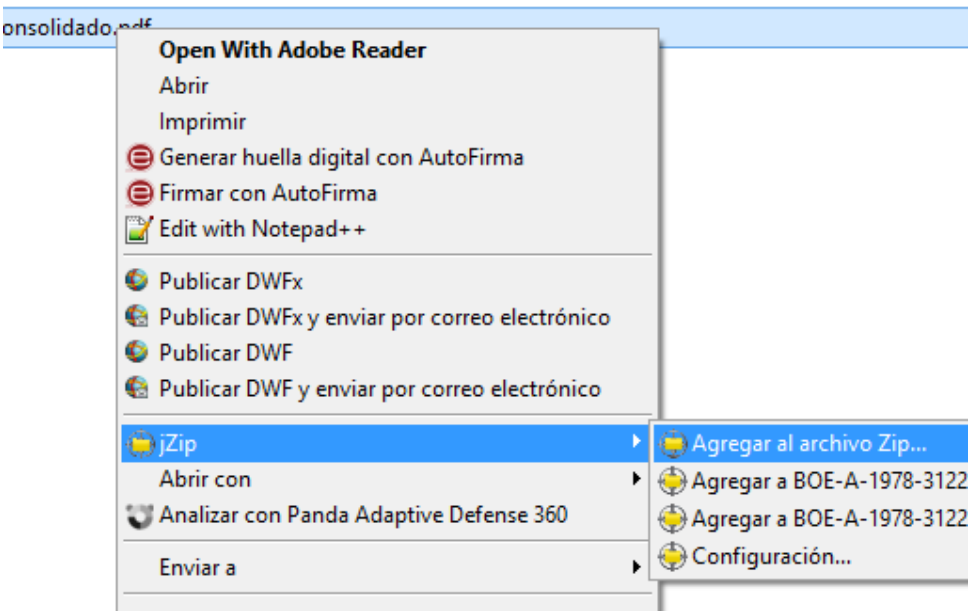
información enviada, limitándose a aquélla que esté debidamente justificada y motivada, y que sea estrictamente necesaria. En los casos de envío de correos a una pluralidad de destinatarios, se deberá utilizar como norma general, el campo de Copia Oculta (CCO), salvo en los casos en los que sea necesario que el destinatario conozca quién más ha recibido ese correo.

- En los casos de uso de **buzones genéricos,** del tipo unidad-x@madrid.org, para el tratamiento de datos personales, el acceso a la documentación debe realizarse únicamente por personal autorizado. Es aconsejable que se establezcan mecanismos que permitan identificar los accesos realizados.
- En caso de que se emplee como medio de comunicación el correo electrónico, el emisor y el destinatario deberán utilizar **cuentas de correo electrónico corporativas**, y nunca correos externos a la Consejería o de uso personal (por ejemplo, correos tipo Gmail).

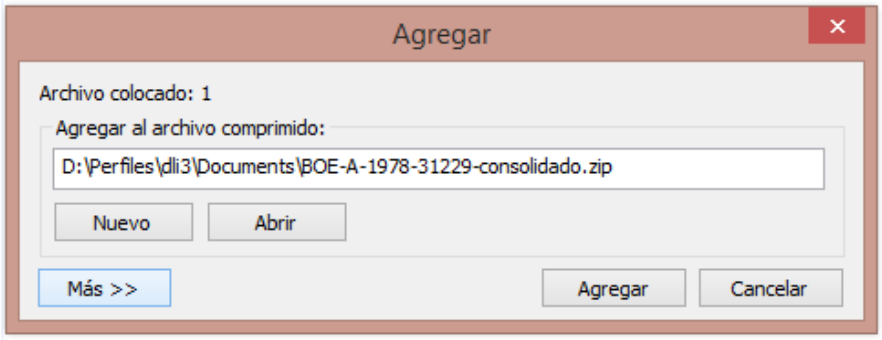
TÉCNICA DE CIFRADO DE ARCHIVOS MEDIANTE LA APLICACIÓN JZIP

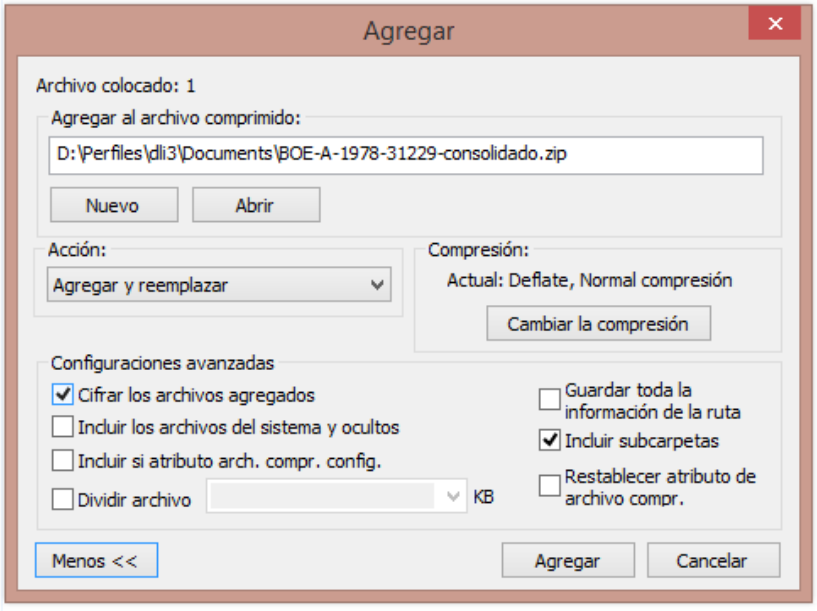
(Presente en la mayoría de los ordenadores personales de la Comunidad de Madrid)

Para cifrar un archivo ubicado en una carpeta del ordenador personal se deberá situar el ratón sobre dicho archivo y pulsar su botón derecho, eligiendo la opción “Agregar al archivo Zip…”



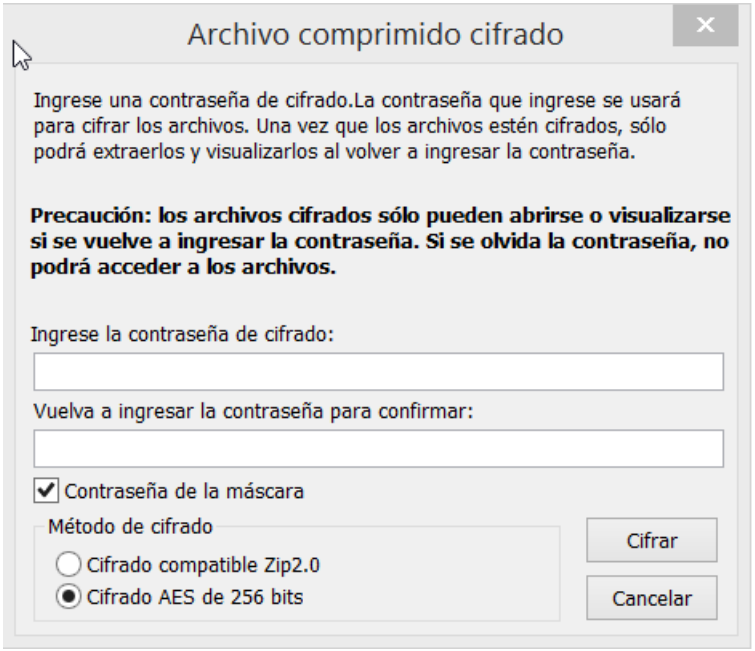
Para que aparezca la opción de cifrado hay que pulsar en el botón “Más >>”





Marcaremos la casilla de la opción “Cifrar los archivos agregados” y pulsaremos el botón “Agregar”, tras lo cual se solicitará la contraseña de cifrado.

Se recomienda marcar la opción “Cifrado AES de 256 bits”, pues es más robusto y confiable, tal y como indica el Centro Criptológico Nacional en su guía STIC 807 (Criptología de empleo en el Esquema Nacional de Seguridad)



Nota: la opción “contraseña de la máscara” está mal traducida al castellano. Debería decir “enmascarar la contraseña”, que se utiliza para que los caracteres de la contraseña no sean visibles, mostrándose en su lugar asteriscos.

2. TRANSPORTE DE DOCUMENTACIÓN

Con frecuencia, en nuestro trabajo diario nos vemos en la necesidad de disponer de acceso a documentos que contienen datos personales fuera de nuestro lugar de trabajo.

En el caso de documentos digitalizados o en formato electrónico, como ya hemos señalado, se aconseja el uso del servicio Cloud de EducaMadrid, para garantizar un acceso seguro previa autenticación por código de usuario y contraseña, así como su compartición de manera segura.

No obstante, si excepcionalmente es preciso transportar los documentos en dispositivos de almacenamiento físico, tales como unidades USB o discos ópticos (CD / DVD), recomendamos que la información se cifre previamente a su almacenamiento en el dispositivo.

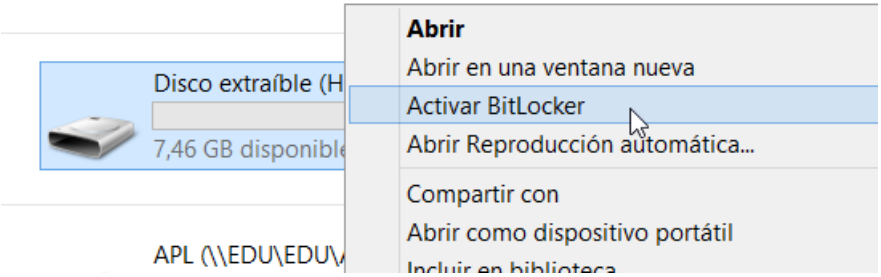
Si se trata de un disco óptico el cifrado puede realizarse fácilmente según se especifica en el apartado anterior, gracias a las herramientas de compresión y cifrado disponibles en los ordenadores personales de la Comunidad de Madrid (jZip).

En el caso de los dispositivos USB se aconseja aplicar la técnica del cifrado al dispositivo de manera integral, de modo que una vez aplicado el cifrado el propio sistema Windows se encargará de cifrar y descifrar los documentos. Tan sólo será necesario establecer

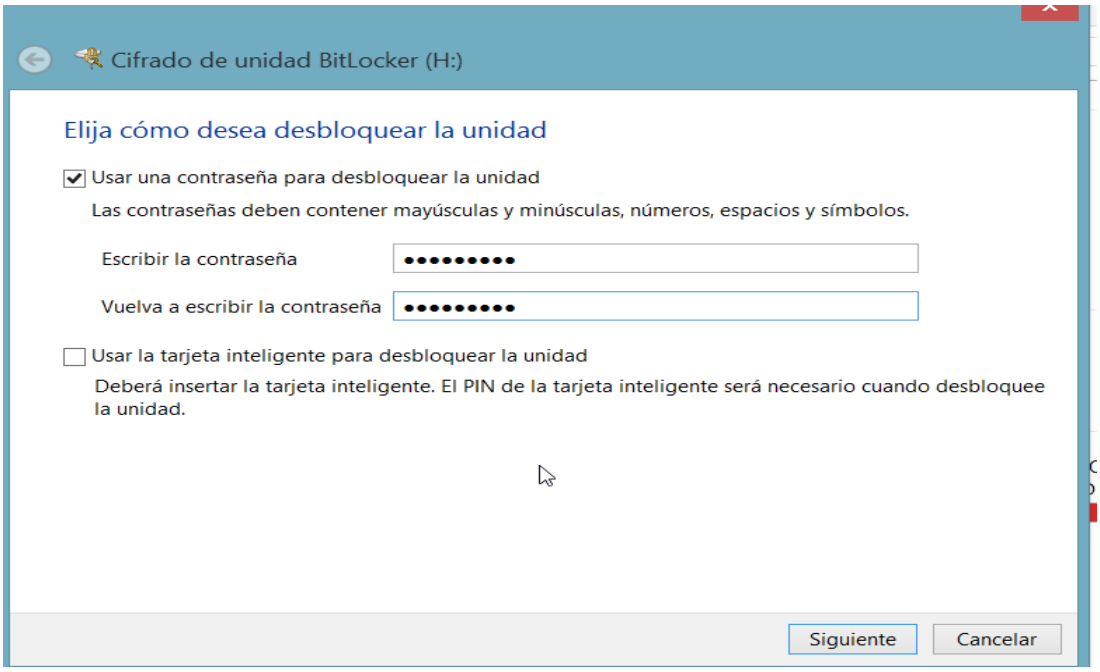
una contraseña que será solicitada siempre en el momento de conexión del dispositivo al ordenador. A continuación se detalla el procedimiento de cifrado.

TÉCNICA DEL CIFRADO AL DISPOSITIVO DE MANERA INTEGRAL

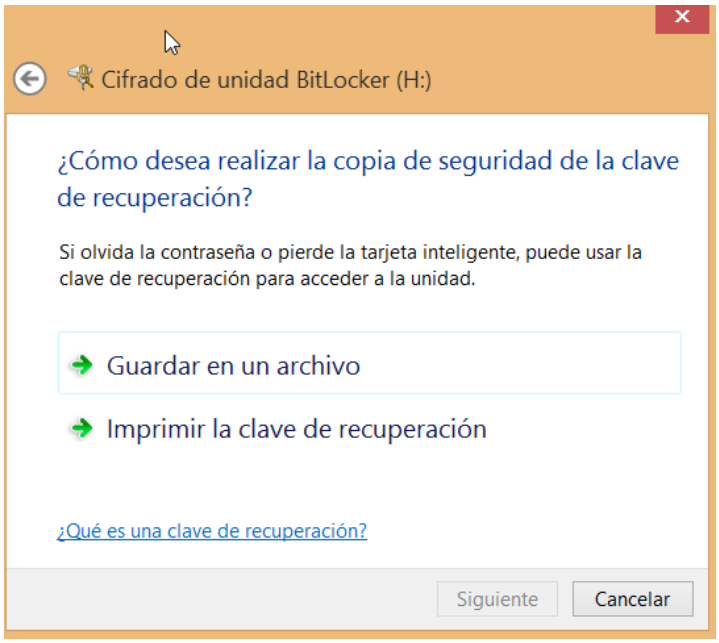
El sistema puede utilizarse en sistemas Windows con versión 8 o superior. Para habilitar el cifrado permanente en un dispositivo USB hay que activar el servicio de cifrado denominado “Bitlocker”, tras situar el ratón encima del dispositivo, pulsando con el botón derecho dicha opción según se muestra a continuación:



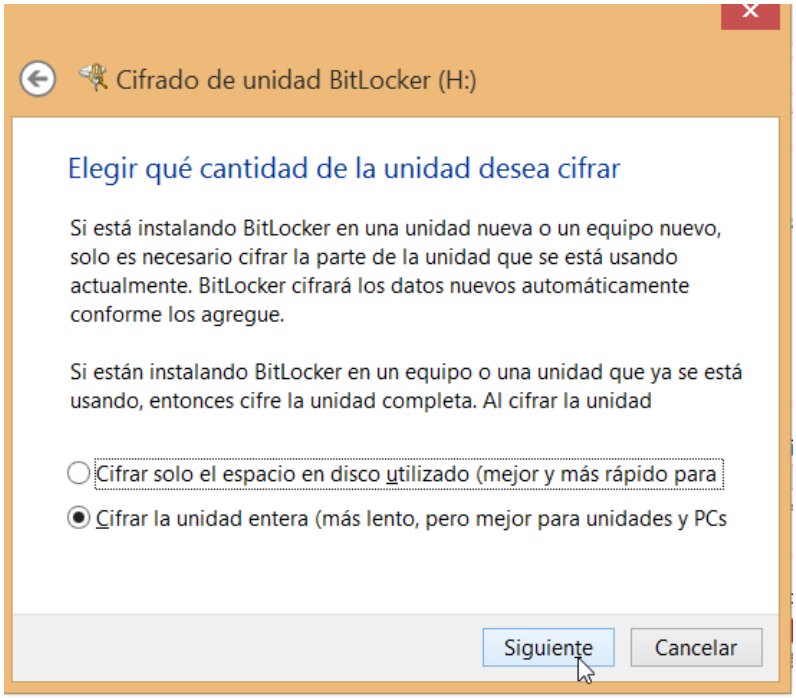
Después se solicita una contraseña que deberá emplearse cada vez que el dispositivo USB se inserte en un ordenador con sistema Windows 8 o superior:



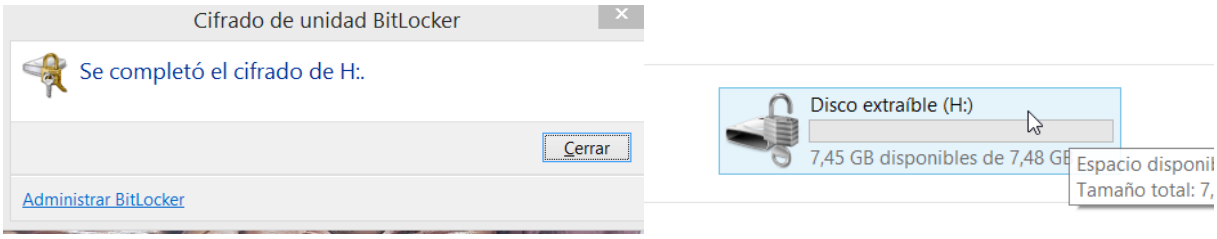
El sistema almacenará dicha clave, y creará otra de recuperación para su uso en caso de olvido de la contraseña principal:



Realizada dicha elección se nos preguntará si deseamos cifrar únicamente la parte que contiene documentos o bien todo el soporte de almacenamiento USB. Se aconseja elegir la segunda opción, como se indica a continuación.

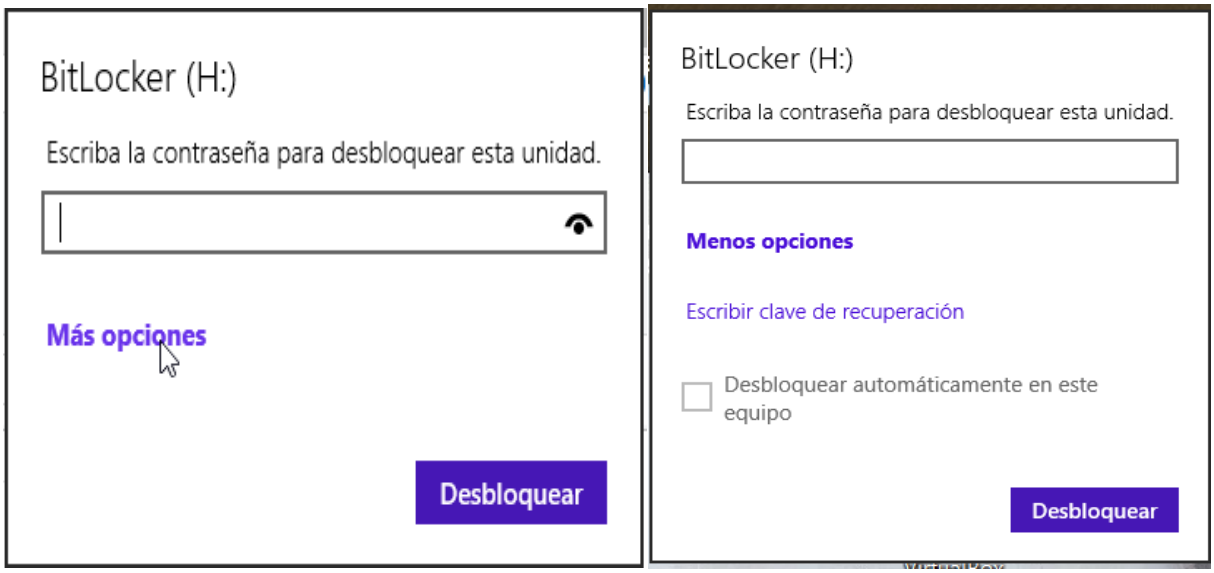


Una vez finalizado el proceso, la unidad USB aparecerá en el sistema con un candado que indica que su contenido está cifrado:



En adelante cada vez que introduzca el dispositivo USB en un ordenador con Windows 8 o superior se le pedirá la contraseña de cifrado.

En caso de olvido de la contraseña principal se requerirá el uso de la contraseña de desbloqueo (o de emergencia). Para ello deberá pulsar en “Más opciones” en el diálogo de desbloqueo y posteriormente elegir la opción “Escribir Clave de Recuperación”



DELEGACIÓN DE PROTECCIÓN DE DATOS

2021