Proteger los datos Es proteger a la gente

GUÍAS DE PROTECCIÓN DE DATOS Y PRIVACIDAD

MERCY CORPS

Cifrado de un archivo

Esta sección aborda un ejemplo básico del cifrado de un archivo con una función de Microsoft disponible en los equipos de Mercy Corps. Hay una serie de factores a tener en cuenta al cifrar un archivo, pero nos centramos en el uso de una contraseña y en el cifrado de un solo archivo. En los siguientes enlaces encontrará recursos que profundizan en el cifrado. Sin embargo, es útil entender la sutil diferencia entre «protección con contraseña» y «cifrado» en lo que refiere a esta guía.

Piense en la protección con contraseña como una caja con un candado. Cuando «protege con contraseña» su documento, lo mete en una caja fuerte electrónica y la cierra con una contraseña: solo quien tiene la contraseña puede abrir la caja. Sin embargo, si la contraseña que elige no es muy fuerte, o si se comparte con la persona equivocada, alguien puede entrar fácilmente a la caja y ver su documento. Por el contrario, el cifrado usa complejos algoritmos para codificar la información, lo que requiere disponer de una clave para descifrarla. Piense en esto como si tomara su documento y lo pasara por una trituradora de papel que asigna una clave especial para volver a armar el documento.

Cuando se combina la protección con contraseña y el cifrado, se duplica la protección. Si alguien consigue descifrar la contraseña de la caja fuerte electrónica, solo podrá ver los trozos de papel triturados si también no tiene la contraseña adecuada. Todas las computadoras de Mercy Corps están cifradas con Microsoft BitLocker. Esto evita que se extraiga y se acceda al disco duro de un equipo de cómputo de Mercy Corps en otro equipo.

☆ Importancia

El cifrado es fundamental porque ayuda a garantizar la privacidad y la seguridad de la información. Sin cifrado, los datos pueden ser interceptados y leídos por cualquiera que tenga acceso a ellos. A la hora de plantearse si cifrar o no los datos, pregúntese: «¿Cuál es el riesgo para los participantes del programa de Mercy Corps, el personal y los socios si se perdieran o fueran robados estos datos?» Una buena regla general es cifrar todo lo que contenga información de identificación personal o confidencial.

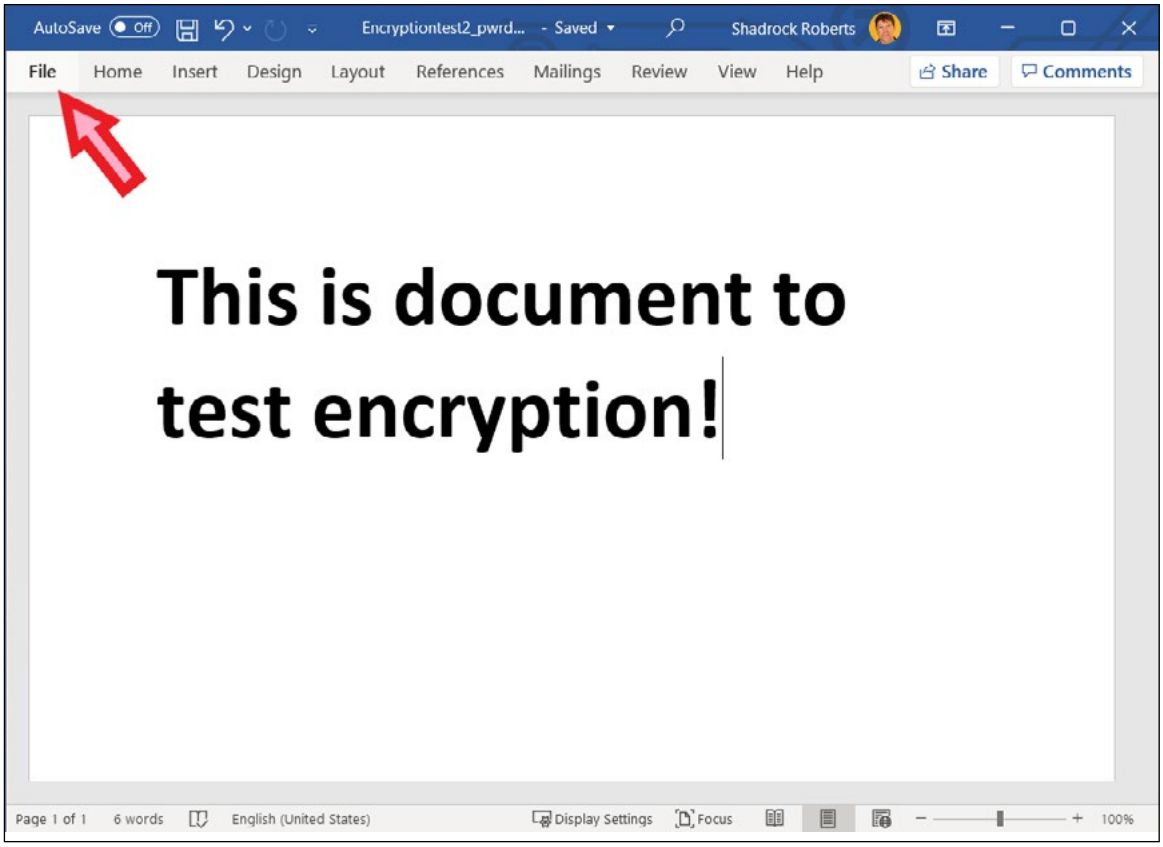
Principios

- Usar sistemas aprobados por Mercy Corps para la transferencia y el almacenamiento de datos cifrados (por ejemplo, Microsoft SharePoint o Google Drive). En caso de duda, pida consejo a su equipo local de TI.
- Cifre los datos confidenciales en todas las fases de su recolección, uso, transmisión y almacenamiento.
- Use contraseñas seguras y no repita las contraseñas. Las listas de contraseñas circulan por Internet y facilitan que alguien con una de sus contraseñas pueda acceder a más de una de sus cuentas o archivos. Es posible que quiera usar un gestor de contraseñas, como Lastpass. Sin embargo, los gestores de contraseñas pueden ser vulnerables a los ciberataques de aplicaciones falsas, por lo que es fundamental que los gestores de contraseñas se usen como parte de un enfoque más amplio para proteger los datos.

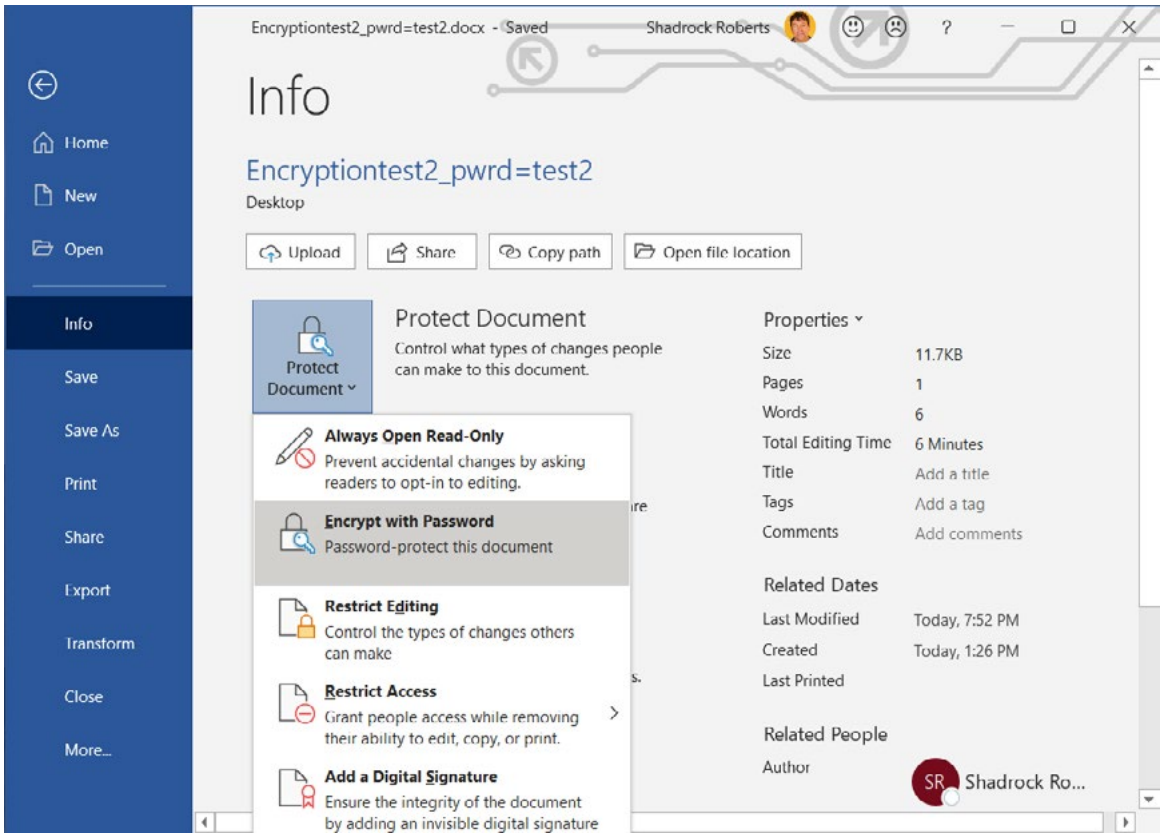
- En un entorno de equipo, el cifrado es tan bueno como el eslabón más débil. Si una sola persona no usa el cifrado, los datos del programa están en peligro. Comunicarlo a su equipo es extremadamente importante: el cifrado no es solo una cuestión de tecnología, sino también de cambio de comportamiento.
- Conozca las leyes que rigen el cifrado en su país. Las leyes locales de varios países (como Sudán, Yemen y Pakistán) ponen límites al software de cifrado. En caso de duda, pida consejo a su equipo local de TI. Por lo general, trabajarán con usted para garantizar que los discos duros de sus equipos estén debidamente cifrados con Intune.

Instrucciones

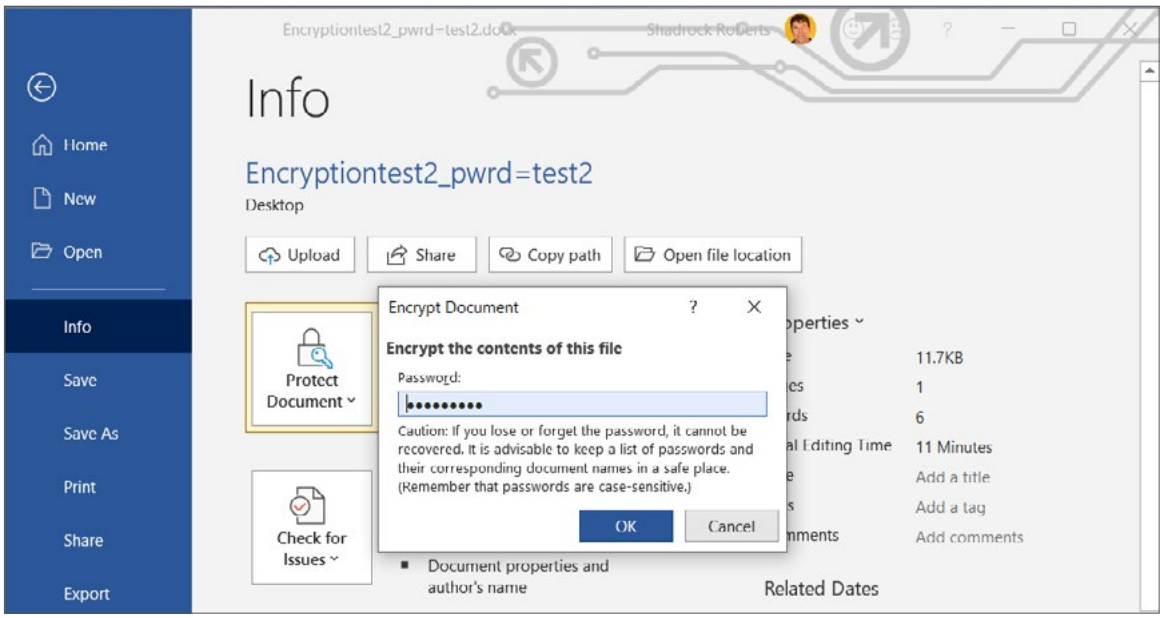
1 Abra el archivo de Word, Excel o PowerPoint que desea cifrar y seleccione el menú **Archivo**.



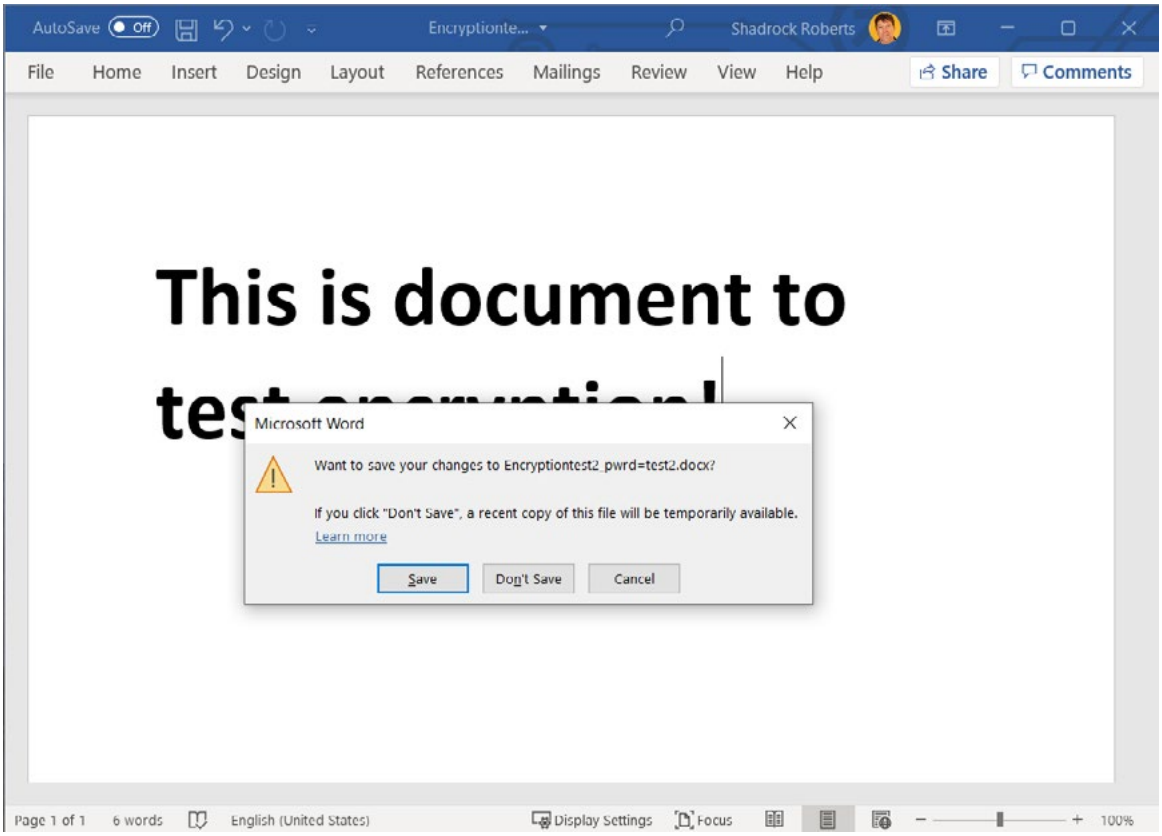
2 Desplácese a **Información** > **Proteger documento** > **Cifrar con contraseña**.



3 Escriba una contraseña, haga clic en **Aceptar** y vuelva a escribirla para confirmarla.



4 Guarde el archivo para que la contraseña surta efecto.



Ahora puede compartir el archivo y la contraseña con quienes requieran el acceso. La mejor práctica es colocar el archivo en un servicio en la nube aprobado por Mercy Corps, como G Suite o SharePoint. Recuerde enviar el enlace del archivo y el de la contraseña por separado. Por ejemplo, puede compartir el archivo con Google Drive (**consulte la sección Uso compartido de archivos**) y generar un aviso de que el archivo fue compartido a través de Google, y luego compartir la contraseña a través de un correo electrónico a un compañero.

Asistencia adicional

- El conjunto de iniciación de datos de la Red de Aprendizaje de Transferencias Monetarias Electrónicas (Electronic Cash Transfer Learning Action Network) ofrece una hoja de consejos para el cifrado (consulte la hoja de consejos n°. 5).
- Electronic Frontier Foundation ofrece un análisis más detallado de las distintas formas de cifrado.
- El Engine Room's Hand-Book of the Modern Development Specialist (Manual del Especialista en Desarrollo Moderno de la Sala de Máquinas) incluye una sección sobre la gestión de los datos que ofrece ideas adicionales de alto nivel sobre el cifrado.

CONTACTO

HEATHER LOVE
Directora, Protección Global de Datos y Privacidad | IT
hlove@mercycorps.org

SHADROCK ROBERTS
Especialista en protección de datos | IT
shroberts@mercycorps.org

Acerca de Mercy Corps
Mercy Corps es una organización global líder impulsada por la creencia de que un mundo mejor es posible. Ante catástrofes y dificultades, en más de 40 países en todo el mundo, nos asociamos para poner en marcha soluciones audaces y ayudar a que las personas triunfen en la adversidad y construyan comunidades más fuertes desde adentro. Ahora y para el futuro.

MERCY CORPS

Sede global
45 SW Ankeny Street
Portland, Oregon 97204
888.842.0842
mercycorps.org

Sede europea
40 Sciences
Edinburgh EH9 1NJ
Scotland, UK
+44.131.662.5160
mercycorps.org.uk