Proteger los datos Es proteger a la gente

GUÍAS DE PROTECCIÓN DE DATOS Y PRIVACIDAD

MERCY CORPS

El siguiente contenido está diseñado para ayudar al personal de Mercy Corps a tener un mejor entendimiento e implementar mejor las prácticas de datos responsables. Reúne varias políticas y documentos de orientación existentes de Mercy Corps junto con algunos tutoriales sencillos y enlaces a otros recursos. La información se puede tomar en conjunto como una guía completa, o se puede usar cada sección como una guía independiente sobre un tema en particular.

Aunque la guía está destinada principalmente al personal de Mercy Corps, y está diseñada para acompañar el Conjunto de herramientas para datos responsables, la publicamos con una licencia abierta para el beneficio de los socios, las organizaciones homólogas y otras personas que necesiten ejemplos de políticas, plantillas e instrucciones para la implementación de prácticas de datos responsables. Puede descargar todo nuestro contenido a través de nuestra página de Github en https://github.com/mercycorps/DPP-guides.

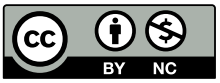
Índice

Citas y agradecimientos

El contenido ofrecido en esta guía forma parte de las buenas prácticas de gestión de datos y del ciclo de vida más amplio de los datos, o las actividades generales de recolección de datos individuales como parte de un programa o respuesta. Los siguientes recursos son excelentes para comenzar a comprender mejor la gestión de los datos de forma responsable. Hemos usado o citado partes de todos estos recursos a lo largo de la Guía y nos referimos a los capítulos o secciones específicas que son más pertinentes para un tema concreto.

- El Conjunto de Herramientas para la Responsabilidad de los Datos de Cash Learning Partnership está diseñado específicamente para los profesionales que reciben su pago en efectivo y vales, pero es una regla de oro en la orientación para los datos responsables. El conjunto de herramientas está disponible en inglés, árabe, francés, y español.
- El conjunto de iniciación a los datos para el personal humanitario de campo de la Red de Aprendizaje sobre Transferencias Monetarias Electrónicas *(Electronic Cash Transfer Learning Action Network)* ofrece una serie de hojas de consejos sobre datos para comprender diversos aspectos de las buenas prácticas de gestión y protección de datos.
- El *Manual de protección de datos en Acciones Humanitarias* del Comité Internacional de la Cruz Roja es una guía detallada de casi todos los aspectos de los datos humanitarios.
- La guía práctica sobre datos de la Federación Internacional de Sociedades de la Cruz Roja y *de la Media Luna Roja* es un excelente recurso de ejercicios, planes de sesiones, listas de comprobación y otros materiales que le ayudarán a organizar conversaciones y actividades con su equipo para desarrollar las actividades de datos responsables.
- El tutorial en línea del Centro de Datos Humanitarios para realizar una evaluación del riesgo de divulgación es un recurso muy específico y técnico, pero es indispensable para una reducción real del riesgo de que se usen los datos para identificar personas.
- El Manual de la Sala de Máquinas del Especialista Moderno en Desarrollo *(Engine Room's Handbook of the Modern Development Specialist)* () es una buena visión general de los datos en el contexto de las actividades de desarrollo internacional.

Licencia



Comprensión de los datos confidenciales

La comprensión de las diferentes clasificaciones de los datos puede ser difícil, pero son una parte importante del trabajo con datos humanitarios. Por ejemplo, ¿cuál es la diferencia entre los datos personales y los datos confidenciales? Determinados tipos de datos pueden requerir un cuidado especial según las leyes regionales o nacionales o las políticas de la organización y pueden presentar diferentes tipos de riesgo tanto para los participantes del programa como para las organizaciones. Los datos confidenciales son una subcategoría de los datos personales y esta sección ofrece una guía detallada para su tratamiento y comprensión.

☆ Importancia

La mayoría de los programas y otras actividades de Mercy Corps recopilan algún tipo de información personal sobre los individuos. En muchos casos, los programas también recopilan información sobre el perfil cultural, orientación sexual, salud o datos biométricos y genéticos del individuo. A estos tipos de datos se los considerarán datos confidenciales y, si se divulgan, se accede a ellos o se comparten de forma inadecuada, podrían dar lugar a:

- daños a una persona, como sanciones, discriminación y amenazas a su seguridad;
- un impacto negativo en la capacidad de Mercy Corps para llevar a cabo sus actividades y una menor confianza o percepción pública.

Es fundamental tomar las medidas necesarias para proteger dichos datos.

Orientación

Esta sección incluye dos documentos:

- La «Guía para el tratamiento de datos confidenciales» le explica que son los datos confidenciales, los términos clave y los aspectos a tener en cuenta a la hora de planificar su recolección, almacenamiento, análisis y difusión.
  - El personal de Mercy Corps puede acceder a la orientación en la biblioteca digital interna de Mercy Corps.
  - Aquí cualquier persona puede acceder a una versión en PDF de las orientaciones en inglés, árabe, español, francés, y ruso.
- Se puede usar la «Plantilla de evaluación de información confidencial (SIA)» con una Evaluación de impacto en la privacidad para documentar todas las salvaguardias adicionales que se emplean para los datos confidenciales. Este documento también establece las diferentes bases jurídicas que se pueden usar para justificar la recolección y el uso de datos confidenciales.

- El personal de Mercy Corps puede acceder a la plantilla de la SIA en la biblioteca digital interna de Mercy Corps.
- Aquí cualquiera puede descargar la plantilla como **un archivo de Microsoft Word** en inglés, árabe, español, francés, y ruso.

Ayuda adicional

La planificación de la recolección o el uso de datos confidenciales debe ser parte de una estrategia más amplia para el ciclo de vida de los datos de un programa o actividad. Hay varios recursos que pueden ayudarle.

- La *guía práctica* sobre datos de la Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja (IFRC) es un excelente recurso de ejercicios, planes de sesiones, listas de comprobación y otros materiales que le ayudarán a organizar conversaciones y actividades con su equipo. En particular, el Módulo 4: Datos Responsables es un buen punto de partida.
- *El Manual de protección de datos en Acciones Humanitarias* del Comité Internacional de la Cruz Roja es una guía detallada de casi todos los aspectos de los datos humanitarios. El capítulo 3 trata específicamente sobre el fundamento jurídico para el tratamiento de datos personales.
- El *conjunto de herramientas para la responsabilidad de los datos* de Cash Learning Partnership está diseñado específicamente para los profesionales que reciben sus pagos con efectivo y vales, pero es una regla de oro en la orientación para los datos responsables. En concreto, *en la hoja de consejos n°. 2, «Diseño y planificación»*, se habla del fundamento jurídico de los datos confidenciales. El conjunto de herramientas está disponible en inglés, árabe, francés, y español.

Evaluaciones de impacto en la privacidad

Esta guía le ayudará a entender la Evaluación de impacto en la privacidad (PIA) e incluye la orientación y la plantilla de la PIA usada en Mercy Corps. La plantilla de la PIA tiene una serie de preguntas que crean un marco para identificar los posibles riesgos para la privacidad relacionados con la recopilación y gestión de datos que forman parte de la implementación de un nuevo programa o tecnología. Una PIA también es importante cuando cambia el contexto de un programa significativamente y hay que considerar nuevos riesgos o escenarios.

La PIA es necesaria siempre que un nuevo programa, proyecto o tecnología implique la recolección o el uso de datos personales o confidenciales.

☆ Importancia

Una PIA permite analizar la manera en que un proyecto concreto o una nueva tecnología afectará la privacidad de las personas implicadas. Una PIA también ayuda a documentar las estrategias de mitigación que protegen la privacidad de los participantes y refuerzan la confianza del público en nuestro trabajo. Una PIA garantiza que los posibles problemas se identifiquen en una fase temprana, cuando su resolución sea más sencilla, menos costosa y no suponga un riesgo para los participantes del programa o del personal.

Principles

Los principios en los que se basa una PIA son similares a los de cualquier uso seguro de los datos personales. A continuación se exponen algunos principios clave adaptados de Cash Learning Partnership (CaLP):

- Identificar los riesgos para la privacidad de las personas.
- Identificar las responsabilidades del cumplimiento de la privacidad y la protección de datos en su organización.
- Demostrar la rendición de cuentas y el cumplimiento de las políticas que protegen a los participantes del programa, a los socios y al personal.
- Garantizar que la organización promueve el derecho a la privacidad en sus actividades humanitarias y actúa como un custodio ético de los datos.

Orientación

El personal de Mercy Corps puede encontrar la Guía de PIA en la Biblioteca Digital. El documento tiene respuestas a las preguntas más frecuentes relacionadas con las PIA y enlaces al archivo interno de Mercy Corps de las PIA completadas para su comparación. La Guía PIA de Mercy Corps está disponible para cualquier persona en inglés, árabe, español, francés, y ruso.

Recuerde:

- Una PIA es un proceso usado para identificar y minimizar los riesgos para la privacidad. ¡Completar un formulario PIA no es el final del proceso! Vuelva a revisar la PIA una vez iniciado el proyecto para asegurarse que no haya cambios que presenten riesgos nuevos. De haberlos, documente los cambios y las nuevas estrategias de mitigación necesarias para minimizar cualquier riesgo nuevo.

- Realizar una PIA implica trabajar con personas de Mercy Corps y, a veces, con organizaciones asociadas y otras para identificar y reducir los riesgos para la privacidad. Por ejemplo, si usa una nueva tecnología, es posible que deba investigar si la empresa con la que trabaja tiene una política de privacidad y las salvaguardias tecnológicas que usa para garantizar la protección de los datos. Es posible que también se deba informar sobre la normativa de privacidad pertinente en su país de actuación. Tres sitios web que puede usar para controlar los datos a nivel nacional y las leyes de privacidad son:
  - Leyes de protección de datos del mundo;
  - La base de datos de la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo de la legislación sobre protección de datos y privacidad en todo el mundo; y
  - La base de datos de One Trust Data Guidance sobre las leyes de privacidad mundiales.

- La comparación de las PIA de programas similares puede ser útil. Puede realizar esta investigación por su cuenta o contactar al equipo de Protección de Datos y Privacidad para obtener ayuda.

Plantillas

El personal de Mercy Corps puede encontrar la Plantilla PIA ampliada en la Biblioteca Digital. La plantilla PIA ampliada está disponible para cualquier persona en inglés, árabe, español, francés, y ruso.

Cada plantilla PIA ampliada incluye cinco casos de uso, que se explican a continuación. Al hacer clic en los enlaces que aparecen a continuación, se accede a una pantalla en la que se pueden descargar las versiones en inglés de cada uno de los casos de uso en formato **.odt** (formato compatible con Microsoft Word y con aplicaciones de código abierto como OpenOffice y LibreOffice) al hacer clic en **Ver en blanco** o en el botón **Descargar**.

- una nueva Política
- un nuevo Proceso o Procedimiento
- un nuevo software o sistema tecnológico
  - Se trata sobre todo de la implementación de nuevos sistemas globales, nacionales o específicos de un equipo.
  - Si está en el proceso de selección o usa un nuevo sistema como parte de un proyecto o programa mayor, use en su lugar la opción de proyecto o programa.

› un nuevo proveedor o socio

- Está pensado principalmente para la validación de las actividades de un proveedor, socio o tercero como parte de una actividad única o de una sola vez.
- Si está en el proceso de selección o usa un nuevo proveedor, socio o a un tercero como parte de un proyecto o programa mayor, use la opción de proyecto o programa.

› un nuevo proyecto o programa

- Esto se puede aplicar a cualquier fase o aspecto de un proyecto o programa.
- *Esta es la opción más completa de la PIA*, e incluye terminología para la selección de nuevos programas o sistemas tecnológicos, o un nuevo proveedor o socio.

Ayuda 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 las PIA (**consulte la hoja de consejos n°. 1**).

› La Oficina del Comisario de Información del Reino Unido ofrece un código de prácticas detallado para la realización de evaluaciones de impacto en la privacidad.

› *El Manual de protección de datos en Acciones Humanitarias* del Comité Internacional de la Cruz Roja es una guía detallada de casi todos los aspectos de los datos humanitarios. El capítulo 5 trata específicamente sobre las evaluaciones de impacto en la privacidad.

Mejores prácticas para el uso compartido de archivos

Esta guía cubre las mejores prácticas para el uso compartido de archivos para los miembros del equipo de Mercy Corps que usan las aplicaciones de G Suite, en particular Google My Drive. Para simplificar esta guía, hablaremos del uso compartido de un solo *archivo*, como una hoja de cálculo. Sin embargo, las mismas opciones están disponibles cuando se comparte una *carpeta* de My Drive.

Nota: Mercy Corps está en proceso de transición a Microsoft 365 para el uso compartido de archivos. Una vez que se hayan establecido las mejores prácticas para esa plataforma, se creará un documento o recurso similar.

☆ Importancia

Hay varias razones por las que es mejor compartir un archivo con Google Drive y enviar un enlace en vez de enviar un archivo adjunto en un correo electrónico.

- **Seguridad:** puede cambiar con facilidad quién tiene permiso para acceder o editar su archivo. También puede establecer que el enlace sea sensible al tiempo, permitiendo el acceso al archivo solo durante un período de tiempo determinado.
- **Control de versiones:** al compartir un archivo alojado en línea, muchas personas tienen acceso a la vez y todos los cambios y comentarios quedarán en un solo archivo. El envío de un archivo como adjunto suele generar múltiples versiones del mismo documento con diferentes nombres de archivo, ediciones, comentarios, etc. ¡El propietario del documento perderá mucho tiempo tratando de compilar todo esto en un solo archivo! El uso de un enlace también garantiza que los destinatarios tengan siempre acceso a la versión más actualizada del documento.
- **Tamaño de los archivos:** Algunos departamentos de TI imponen restricciones al tamaño de los archivos adjuntos que se permiten. El envío de un enlace permite el uso compartido de archivos de cualquier tamaño.
- **Edición sencilla:** Los archivos compartidos como documentos de Google en Drive, Microsoft Word en OneDrive o formatos similares le permiten al destinatario abrir el documento e interactuar con él en un navegador web: no es necesario que tenga la versión más reciente de un determinado tipo de software.

Principios

Siempre que comparta documentos, debe tener en cuenta lo siguiente:

- **Considere cuidadosamente la persona que creará el archivo o carpeta, la persona que será su propietario/administrador y quién tendrá acceso a él. Si los contratistas a corto plazo crean y administran archivos, ¡existe el riesgo de que los archivos o el acceso se vayan con los contratistas cuando se vayan!**
  - Solo otorgue el acceso a aquellos que necesitan el archivo.

- Los contenidos confidenciales, privados o de información de identificación personal (PII) deben tener siempre un acceso restringido. Si no puede determinar si el contenido debe ser restringido o cómo hacerlo, solicite ayuda al Departamento Jurídico o al equipo de Protección de Datos y Privacidad.

› Use el nivel de permisos adecuado.

- Consideremos un ejemplo en el que hay que crear un nuevo proyecto modelo. Lo más probable es que tenga acceso completo solo el equipo responsable de la creación del modelo. Cuando llegue el momento de recibir comentarios de otros, conceda permisos adicionales que solo permitan ver o comentar.
- Tenga mucho cuidado a la hora de otorgar acceso a los miembros del equipo que por accidente usen sus cuentas personales de correo electrónico. En lugar de otorgar acceso a una cuenta de correo electrónico personal, conceda acceso a su cuenta de Mercy Corps y pida al miembro del equipo que inicie sesión con esas credenciales.

› Los permisos cambian con el tiempo.

- Si solo va a trabajar con alguien durante un corto periodo de tiempo o con personas ajenas a Mercy Corps, considere la posibilidad de dar permisos temporales. Si más tarde se olvida de eliminar el acceso, una fecha de vencimiento garantizará que se suspenda el acceso en el momento adecuado.
- Revise periódicamente la lista de personas que tienen acceso a sus archivos, carpetas o unidades compartidas para garantizar que elimina el acceso a los miembros del equipo que cambiaron de función o que ya no trabajan en Mercy Corps.

› Los contenidos de riesgo requieren pasos adicionales.

- La información de identificación personal (PII), la información de identificación demográfica (DII) u otros tipos de datos personales están protegidos por múltiples leyes de protección de datos. Antes de compartir datos personales, compruebe los requisitos legales para compartir la información con otros. El intercambio inadecuado de datos personales puede poner en peligro a los participantes del programa, donantes, socios y miembros del equipo de Mercy Corps. Si tiene preguntas sobre los datos personales o la legislación de protección de datos, envíe un correo electrónico al equipo de Protección de Datos y Privacidad en dataprotection@mercycorps.org.
- Si la información se considera confidencial o de propiedad de la empresa, compártala solo con las partes necesarias y considere la posibilidad de otorgar un acceso temporal.
- Si la persona que recibe el archivo trabaja en un lugar inseguro, o si el contenido incluye datos personales, considere cifrar el archivo o protegerlo con una contraseña. Consulte las secciones de cifrado y desidentificación para ver ejemplos de cómo hacerlo.

› Nunca mueva los archivos sin el permiso del propietario.

- ¡Mover los archivos puede alterar quién tiene acceso y hacer imposible que otros encuentren el archivo! Consulte siempre con el propietario del documento antes de mover un archivo compartido a una nueva ubicación.

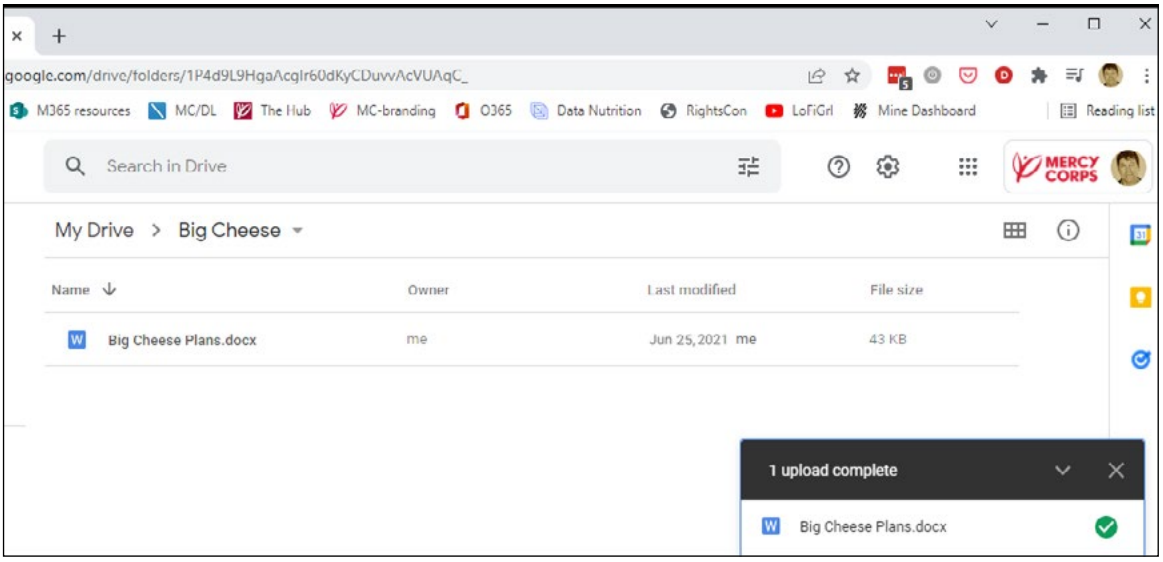
Uso compartido de archivos: GDrive

A continuación, se presenta un ejemplo del uso compartido de un archivo con las mejores prácticas en Google Drive. Imagine que es el año 2020 y que Mercy Corps está trabajando con un consultor (PNW Rocks), para crear materiales para una iniciativa nueva e importante de Mercy Corps, cuyo nombre en clave es Big Cheese. El proyecto Big Cheese no se anunciará públicamente hasta julio de 2021, por lo que es importante limitar el acceso al archivo. Para empezar, convendría que se colabore en los próximos pasos del proyecto con un archivo llamado «Big Cheese Plans».

Instructions

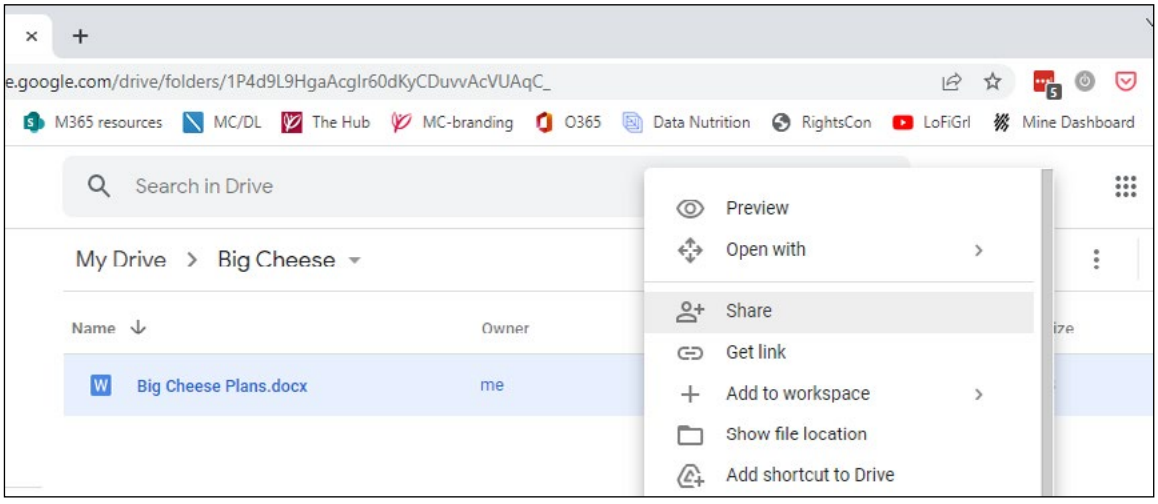
Paso 1: cargar

Suba el archivo a My Drive.



Paso 2: compartir

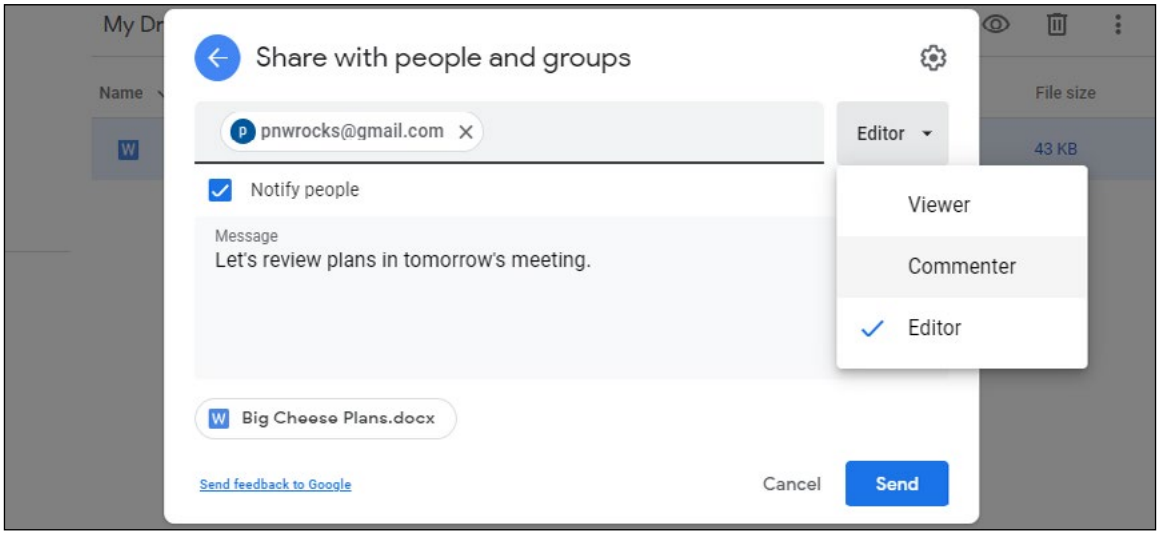
Para compartir el archivo, haga clic con el botón derecho del mouse en el archivo y luego en **Compartir**.



- Solo otorgue el acceso a aquellos que necesitan el archivo. Cuando comparte un archivo en My Drive, la configuración por defecto es **Restringido** (a personas o grupos), que es la mejor práctica. ¡Recuerde que el contenido confidencial, privado o de información de identificación personal (PII) debe tener siempre acceso restringido!
- La opción **Cualquiera con el enlace** solo se debe usar para archivos que no contengan información confidencial y estén abiertos al público. Si se usa la opción Cualquiera con el enlace en un archivo con datos confidenciales privados, personales o financieros, se podría compartir fácil y accidentalmente y poner a Mercy Corps en riesgo legal inmediato y facilitar a los malos actores el uso de la información con fines delictivos.

Paso 3: seleccionar el nivel de acceso

Ingrese la dirección de correo electrónico de la persona con la que desea compartir, y luego elija el nivel de acceso. Google establece por defecto el acceso de **Editor**, que solo es apropiado para los miembros del equipo que necesitan acceso completo al documento. Si desea solicitar la opinión de los interesados, elija **Espectador** o **Comentarista**. La mejor práctica es notificar a la persona, y agregar un mensaje, explicando el motivo por el que compartió el archivo. Para notificar, deje marcada la casilla **Notificar a las personas**. Cuando haya terminado con los cambios, haga clic en **Enviar**.

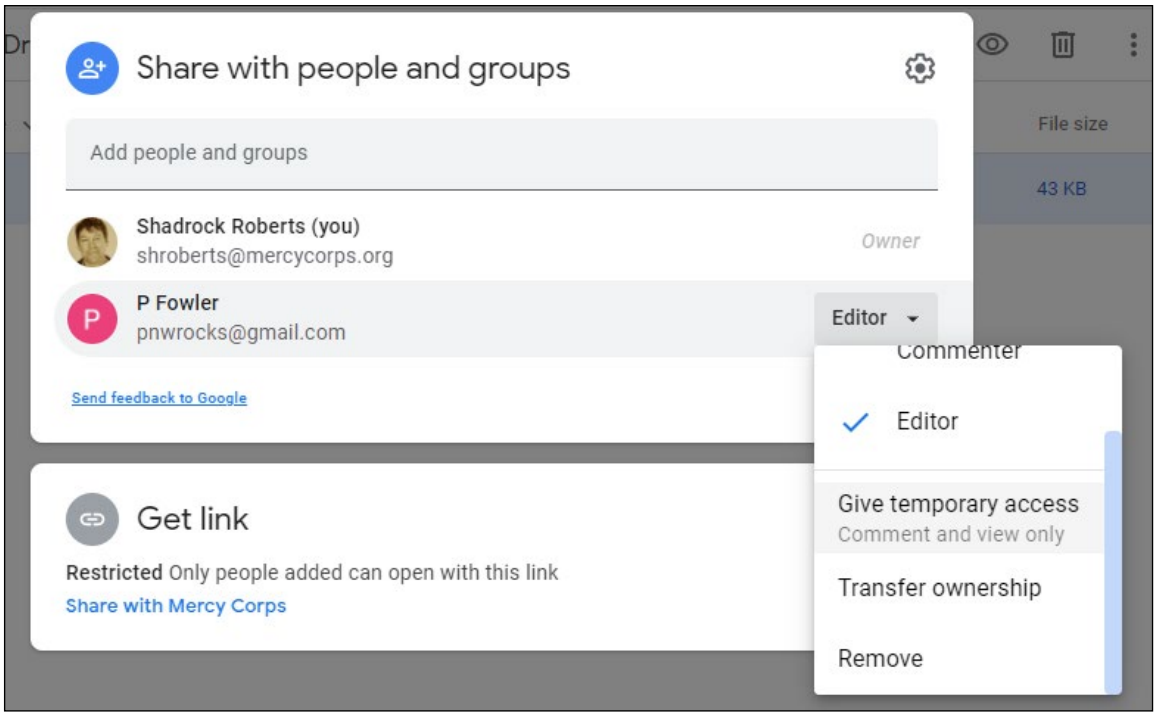


Otra opción es enviar un correo electrónico separado con un enlace al archivo. Para notificar por separado por correo electrónico, desmarque la casilla **Notificar a las personas**. Después de hacer clic en Listo, haga clic con el botón derecho del mouse en el archivo y elija **Obtener enlace**. En la nueva ventana emergente, haga clic en el botón **Copiar enlace** y péguelo en su correo electrónico.

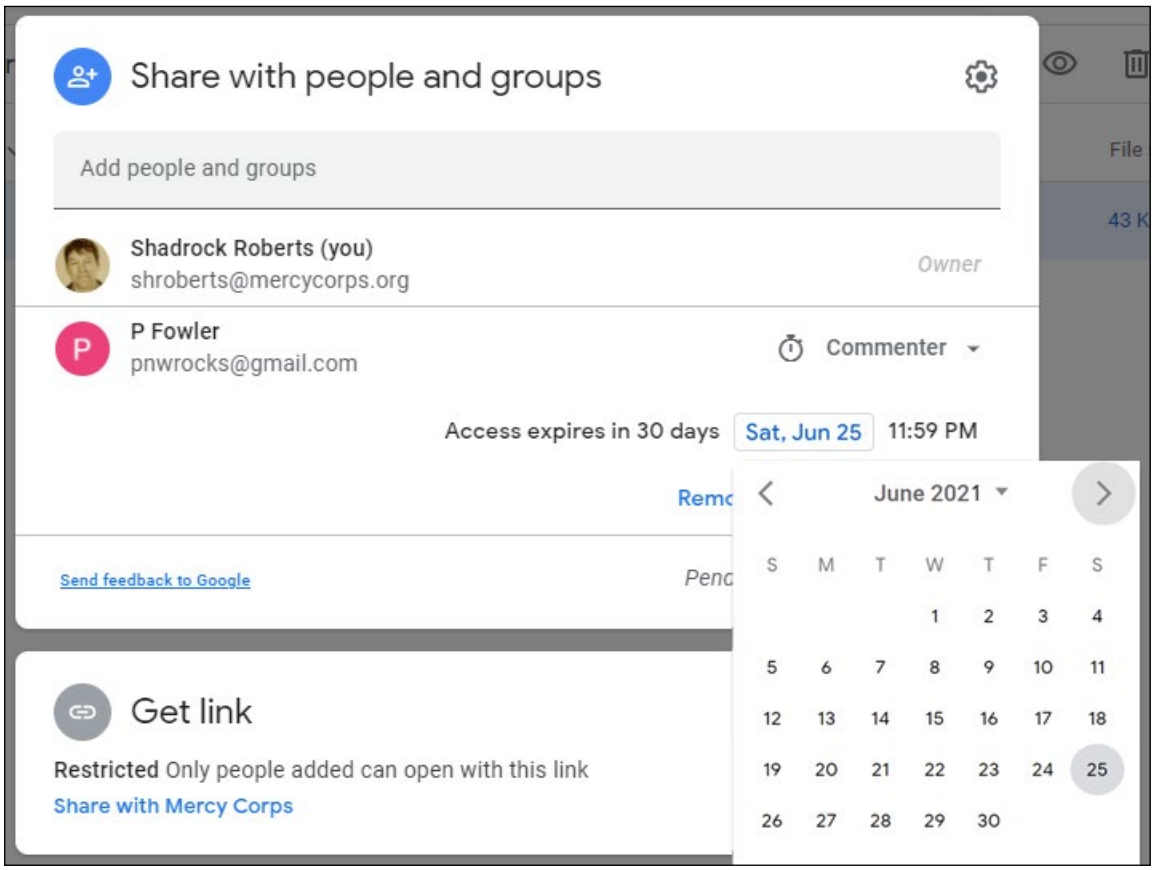
- Para obtener más información sobre los niveles de acceso, visite Compartir y colaborar en My Drive.
- Si restringe un archivo y alguien con acceso comparte el enlace a otra persona, no tendrá acceso automáticamente a ese contenido en Google Drive. En su lugar, verán una página web que le permitirá solicitar el acceso. La solicitud de acceso se dirigirá al propietario del archivo. Debe revisar las solicitudes de acceso, y los que reciben las solicitudes de acceso no deben simplemente otorgar permiso a todas y cada una de las solicitudes, sin revisar las notas y consideraciones anteriores.

Paso 4: acceso temporal

Una vez que se otorgó el permiso, se puede acortar el periodo de uso compartido. Para limitar el acceso, vuelva a hacer clic con el botón derecho del mouse en el archivo y haga clic en **Compartir**. Busque la dirección de correo electrónico que acaba de compartir y haga clic con el botón derecho en el nivel de acceso. Verá que aparecen nuevas opciones; seleccione **Dar acceso temporal**.



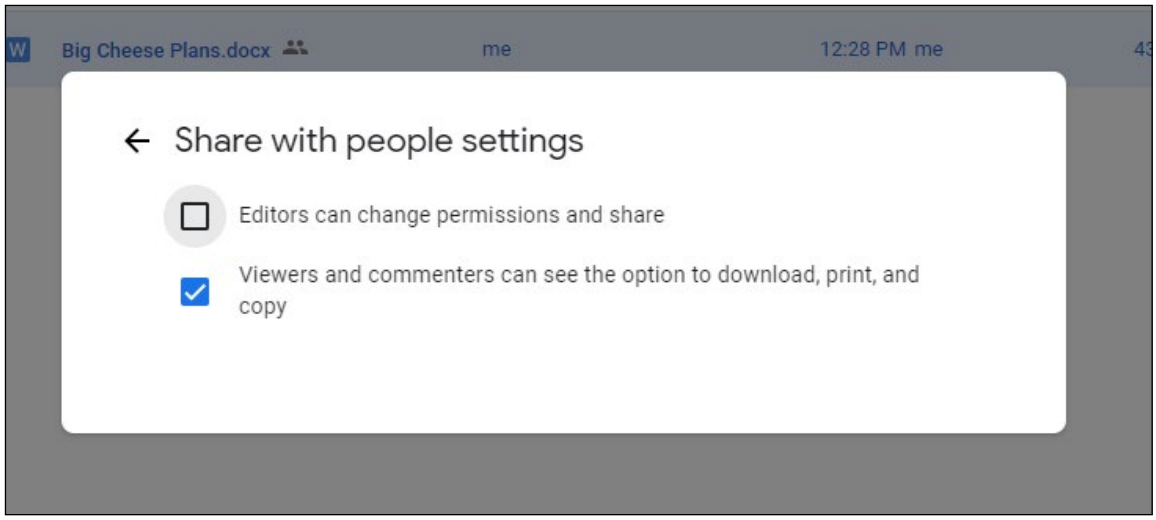
Aparecerá un calendario. Navegue hasta el mes en el que debe vencer el acceso y haga clic en la fecha correspondiente.



Desaparecerá el calendario y cambiará la fecha de la pantalla. Una vez que puede ver que el acceso vencerá en la fecha correcta. Haga clic en **Guardar**.

Paso 5: opciones adicionales

Si le preocupa que otras personas realicen acciones inapropiadas con el contenido, hay opciones adicionales disponibles en la pantalla de configuración. Se puede acceder a la configuración de los archivos desde el icono del engranaje en la parte superior derecha de la ventana de uso compartido. Haga clic en el engranaje y verá las opciones para restringir el uso compartido o desactivar la opción de descargar, imprimir o copiar. Para cualquier función que desee desactivar, simplemente desmarque la casilla. El archivo se actualizará rápidamente, guardando la nueva configuración.



- Para saber más, visite Restringir las opciones de uso compartido en Drive.

Consideraciones adicionales

- No coloque archivos confidenciales dentro de carpetas que sean ampliamente compartidas. Los permisos de las carpetas compartidas se extienden a cada archivo y subcarpeta, por lo que cualquier persona con permiso para la carpeta principal podrá acceder a su archivo confidencial. En su lugar, mueva su archivo confidencial a una nueva ubicación, fuera de la estructura de carpetas compartidas más grande.
- Una vez que se haya compartido un archivo, puede tener la opción **Hacer una copia** o **Mover** el archivo a otra ubicación. ¡Nunca mueva un archivo sin el permiso del propietario!
- Si necesita ver el archivo en My Drive o en una ubicación secundaria, la mejor práctica es usar la opción Agregar acceso directo a la unidad.
- Si se hace una copia del archivo, o se mueve el archivo, tenga en cuenta que no tendrá los mismos permisos que el archivo original a menos que establezca explícitamente esos permisos.

Esta guía no cubre el uso compartido de archivos en las unidades compartidas de Google, ni las plataformas externas para el uso compartido de archivos. Para obtener más información al respecto, visite la página de Google sobre las mejores prácticas para las unidades compartidas o sobre la gestión de las unidades compartidas. Cada una de estas páginas está disponible en varios idiomas: desplácese hasta el final de la página para seleccionar su idioma.

La mejor manera de controlar el acceso a los archivos con Drive es crear un grupo de Google y asignar permisos a los miembros del grupo. Los grupos de Google no solo sirven para enviar correos electrónicos; los grupos son herramientas potentes y cómodas para gestionar los permisos de carpetas y archivos. Más información sobre Grupos de Google.

Si su proyecto requiere el uso de aplicaciones fuera de G Suite, anime a su equipo a descargar Google Drive para escritorio. Este programa le permite ver cualquier documento de My Drive o de las unidades compartidas como si estuvieran en su computadora, incluso sin conexión, y sin tener que descargar el elemento o convertirlo a un formato de Google.

Ayuda adicional

Cómo y con quién compartirá datos debe ser parte de una estrategia más amplia para el ciclo de vida de los datos de un programa o actividad. Hay varios recursos que pueden ayudarle.

- La *guía práctica* sobre datos de la Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja (IFRC) es un excelente recurso de ejercicios, planes de sesiones, listas de comprobación y otros materiales que le ayudarán a organizar conversaciones y actividades con su equipo. En particular, el Módulo 7: Uso compartido de datos es un buen punto de partida.
- *El Manual de protección de datos en Acciones Humanitarias* del Comité Internacional de la Cruz Roja es una guía detallada de casi todos los aspectos de los datos humanitarios. El capítulo 2 trata específicamente del uso compartido de datos.
- El *conjunto de herramientas para la responsabilidad de los datos* de Cash Learning Partnership está diseñado específicamente para los profesionales que son pagados con efectivo y vales, pero es un estándar de oro en la orientación para los datos responsables. Consulte especialmente la *hoja de consejos n°. 6, «Compartir datos»*. El conjunto de herramientas está disponible en inglés, árabe, francés, y español.

Desidentificación de los datos

Esta guía ofrece un ejemplo de eliminación de información de identificación personal (PII) de un conjunto de datos. Hay varias formas de «desidentificar» los datos, lo que hace referencia a las actividades o métodos de tratamiento que funcionan para evitar que se revele la identidad de la persona registrada. Dos tipos comunes de desidentificación son la «anonimización» y la «seudonimización».

La anonimización es el proceso por el que los datos personales se convierten en anónimos, de modo que una persona (o «persona registrada») deja de ser identificable: es un cambio permanente de los datos. Los métodos más comunes incluyen la eliminación de la información de identificación personal o la codificación de los valores de ciertos conjuntos de PII.

> Ejemplo: imagine que una organización tiene datos de encuesta que tienen campos para el nombre, el número de identificación nacional, el nombre de la aldea, la afiliación étnica, la edad, el nivel educativo y los indicadores de salud. En este caso, eliminar el nombre y el número de identificación nacional sería el primer paso para anonimizar los datos, ya que estos «atributos directos» son datos personales que identifican directamente a un individuo. Se mantendrían los «atributos indirectos» del nombre del pueblo, la afiliación étnica, la edad, el nivel educativo y los indicadores de salud.

Sin embargo, aunque algunos atributos parezcan «anónimos» pueden no serlo. Si la encuesta se realizó en una aldea muy pequeña en el que solo dos residentes se identifican como de una determinada filiación étnica, y cada uno de ellos tiene una edad diferente, ¡el uso de esos dos atributos indirectos podría permitir identificar a esas personas! El proceso por el que se examinan todos los atributos para reducir el riesgo de reidentificación de una persona registrada se denomina Control de divulgación estadística. El primer paso en este proceso es una evaluación del riesgo de divulgación y el Centro de Datos Humanitarios tiene un tutorial en línea para realizar una evaluación del riesgo de divulgación.

La seudonimización, por su parte, describe el tratamiento de datos personales de manera que estos ya no puedan atribuirse a una persona registrada específica sin el uso de información adicional, como un código clave.

> Ejemplo: imagine que una encuesta tiene su nombre, dirección de correo electrónico, edad, nacionalidad y lugar de trabajo. La seudonimización toma los datos que son identificables específicamente sobre usted (su nombre, dirección de correo electrónico, edad) y los hace inaccesibles y los separa de los datos no identificables, como su nacionalidad. Los datos seudónimos se pueden volver a reunir en algún momento para que toda la información se pueda vincular a una fuente o persona concreta. Por ello, la seudonimización requiere que la información adicional se conserve por separado y esté sujeta a medidas técnicas y organizativas que garanticen que los datos personales no se atribuyan a la persona registrada.

¿Debe elegir la anonimización o la seudonimización?

La anonimización será generalmente más segura y reducirá el riesgo de exponer la PII. Sin embargo, a veces esto puede hacer que los datos sean demasiado generales, lo que puede hacer que no sean útiles para

programas de asistencia con vales de dinero. En el caso de los programas de salud que implican vacunas u otros tratamientos, contactar a las personas para el seguimiento del tratamiento puede ser importante. En ambos casos, la seudonimización sería la mejor opción, ya que siempre se pueden recomponer los datos para identificar a un individuo cuando sea necesario.

No hay una respuesta única y correcta sobre cuándo elegir un método en lugar de otro, y es importante entender el motivo por el que se recolectaron los datos, los riesgos potenciales asociados a la conservación de esos datos y las necesidades del programa, antes de elegir cómo desidentificar sus datos.

También es importante entender que las técnicas usadas tanto para anonimizar los datos como para hackearlos son cada vez más sofisticadas y que incluso los datos desidentificados no son siempre cien por ciento seguros. En caso de duda, contacte a su equipo de datos o de TI para obtener ayuda.

☆ Importance

Las recientes vulneraciones de datos en el Comité Internacional de la Cruz Roja, los hackeos del correo electrónico en la Agencia de los Estados Unidos para el Desarrollo Internacional, y el intercambio inadecuado de datos por parte del Alto Comisionado para los Refugiados de las Naciones Unidas muestra todas las formas en que los datos humanitarios están en riesgo. Los datos procedentes de las encuestas de hogares, las evaluaciones de necesidades y otras formas de microdatos constituyen un volumen de datos cada vez más importante en el sector humanitario. Este tipo de datos es fundamental para determinar las necesidades y perspectivas de los participantes del programa y de las comunidades en las que trabajamos, pero estos datos también presentan riesgos. La compresión sobre la evaluación y la gestión de la confidencialidad de estos datos es esencial para garantizar que se usen de forma segura, ética y eficaz en diferentes contextos de respuesta.

Algunas de las ventajas de usar datos anonimizados frente a los datos personales son:

- protección contra la divulgación indebida de datos personales;
- se aplican menos restricciones legales a los datos anonimizados; y
- permite a las organizaciones crear datos abiertos o de acceso público sin dejar de cumplir sus obligaciones de protección de datos.

Principios

La desidentificación de los datos forma parte del tratamiento de datos, y el tratamiento de datos personales realizado por las organizaciones humanitarias debe cumplir los siguientes principios.

- **Imparcialidad y legalidad del tratamiento:** los métodos deben cumplir con la legislación o las políticas regionales, nacionales o locales que pueden limitar los datos que se pueden desidentificar y el uso de determinadas tecnologías. Todo tratamiento de datos personales debe ser transparente para las personas registradas.
- **Limitación de la finalidad:** las organizaciones humanitarias deben determinar y establecer los fines específicos para los que se tratan los datos. Estos fines deben ser explícitos y legítimos.
- **Proporcionalidad:** garantiza que cada actividad concreta relacionada con el tratamiento de datos personales sea la adecuada para el objetivo declarado. Por ejemplo: ¿solo se recopila la cantidad mínima de datos necesaria? ¿Existen medidas técnicas y organizativas adecuadas para reducir los riesgos asociados al tratamiento de datos?

- **La tecnología cambia:** los nuevos conjuntos de datos y las nuevas herramientas para analizarlos cambian y avanzan rápidamente, al igual que los medios por los que se hackean o roban los datos. Es importante comprender los riesgos nuevos y emergentes para sus datos y seguir ajustando sus métodos y prácticas en consecuencia.

Seudonimización

Este es un ejemplo de una forma de desidentificar datos en una hoja de cálculo. Hay una gran variedad de métodos de desidentificación y este ejemplo usa un «código clave» para eliminar la información de identificación personal que se encuentra en los identificadores directos y guardarla en un archivo separado. La información de identificación personal (PII) es información que se puede usar para identificar a un individuo. Los ejemplos más comunes son el nombre, dirección, número de teléfono, fecha de nacimiento y número de seguro social o de identificación nacional.

Instrucciones

Puede seguir estas instrucciones de seudonimización para ver un ejemplo básico de seudonimización de un conjunto de datos. El ejercicio usa un conjunto de datos de muestra que se encuentra en la carpeta de datos de la guía en línea.

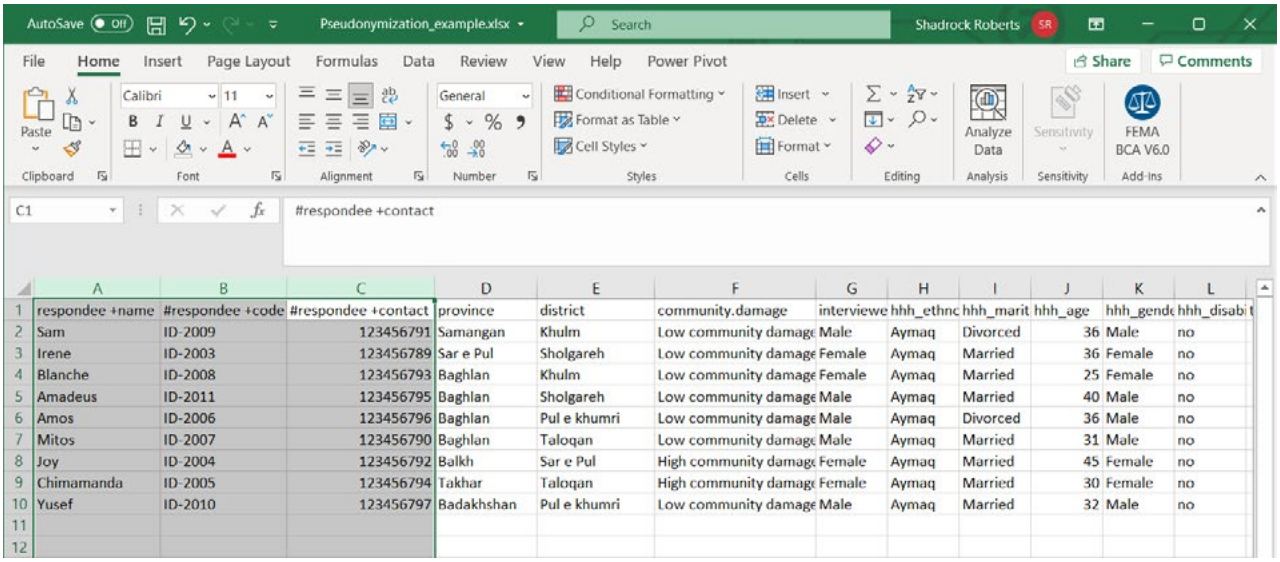
Una vez que terminado la seudonimización de los datos de muestra, se puede continuar con el tutorial del Centro de Datos Humanitarios para realizar una evaluación del riesgo de divulgación.

Paso 1: identificar la PII

Comience por identificar la PII en los datos. Lo ideal es que disponga de metadatos (datos o un documento que defina sus datos) para ayudarle a comprender los campos que tienen PII. En los datos de la muestra, hay tres columnas que tienen posible PII:

- **# de respondedor +nombre** parece incluir un nombre.
- **# de respondedor + código** probablemente tiene un número de identificación de algún tipo.
- **# de respondedor + contacto** posiblemente tiene un número de teléfono móvil

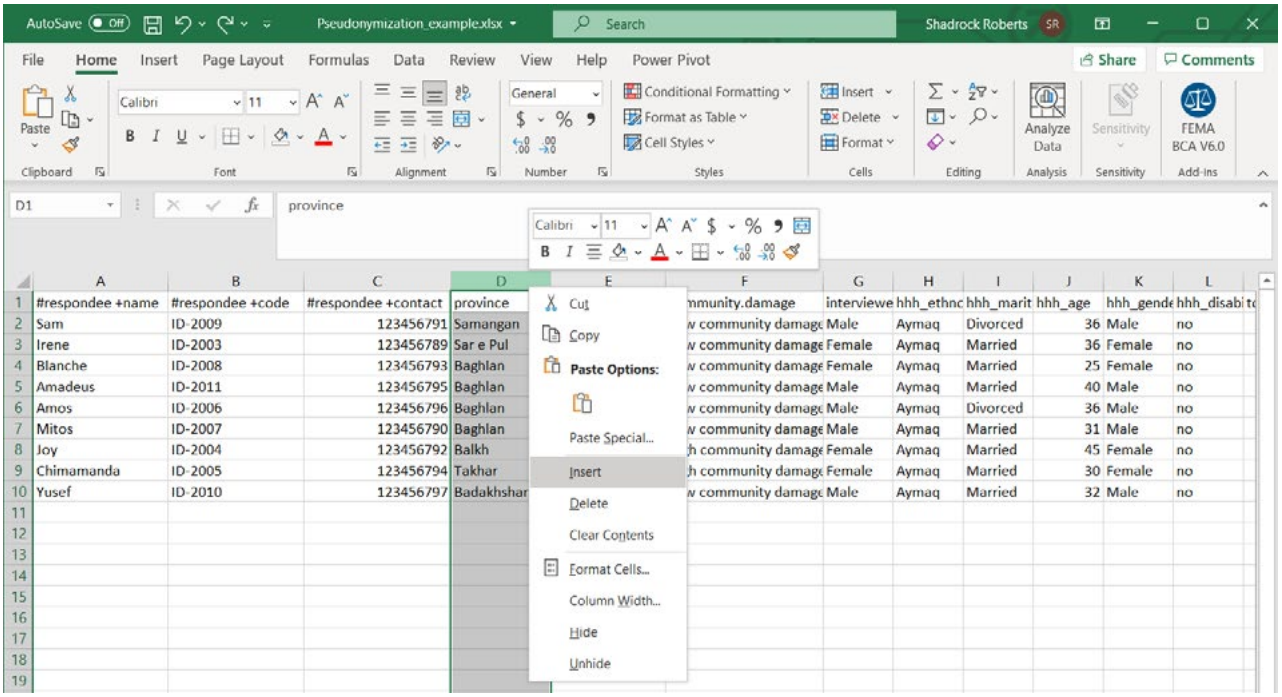
Cada uno de estos identificadores directos usa el Lenguaje de Intercambio Humanitario para etiquetar los datos.



	A	B	C	D	E	F	G	H	I	J	K	L
1	respondee +name	#respondee +code	#respondee +contact	province	district	community.damage	interviewe	hhh_ethnc	hhh_marit	hhh_age	hhh_gende	hhh_disabi
2	Sam	ID-2009	123456791	Samangan	Khulm	Low community damage	Male	Aymaq	Divorced	36	Male	no
3	Irene	ID-2003	123456789	Sar e Pul	Sholgareh	Low community damage	Female	Aymaq	Married	36	Female	no
4	Blanche	ID-2008	123456793	Baghlan	Khulm	Low community damage	Female	Aymaq	Married	25	Female	no
5	Amadeus	ID-2011	123456795	Baghlan	Sholgareh	Low community damage	Male	Aymaq	Married	40	Male	no
6	Amos	ID-2006	123456796	Baghlan	Pul e khumri	Low community damage	Male	Aymaq	Divorced	36	Male	no
7	Mitos	ID-2007	123456790	Baghlan	Taloqan	Low community damage	Male	Aymaq	Married	31	Male	no
8	Joy	ID-2004	123456792	Balkh	Sar e Pul	High community damage	Female	Aymaq	Married	45	Female	no
9	Chimamanda	ID-2005	123456794	Takhar	Taloqan	High community damage	Female	Aymaq	Married	30	Female	no
10	Yusef	ID-2010	123456797	Badakhshan	Pul e khumri	Low community damage	Male	Aymaq	Married	32	Male	no
11												
12												

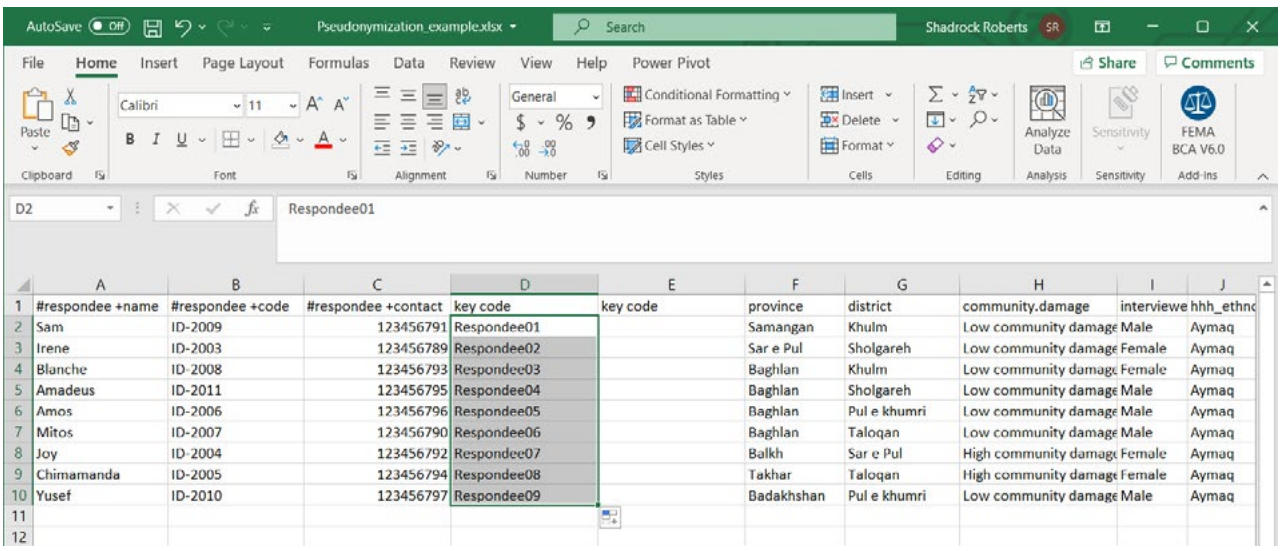
Paso 2: crear nuevas columnas para el código clave

Usaremos un código clave, un valor que generamos, para separar la PII. Como los identificadores directos están todos agrupados, crearemos dos nuevas columnas entre las columnas C, **# de respondedor +contacto** y la columna D, **provincia**. En Excel, lo hacemos al resaltar una columna a la derecha de donde queremos insertar nuevas columnas, hacemos clic con el botón derecho en la columna y seleccionamos **Insertar**. Vuelva a repetir este proceso para crear otra columna vacía.



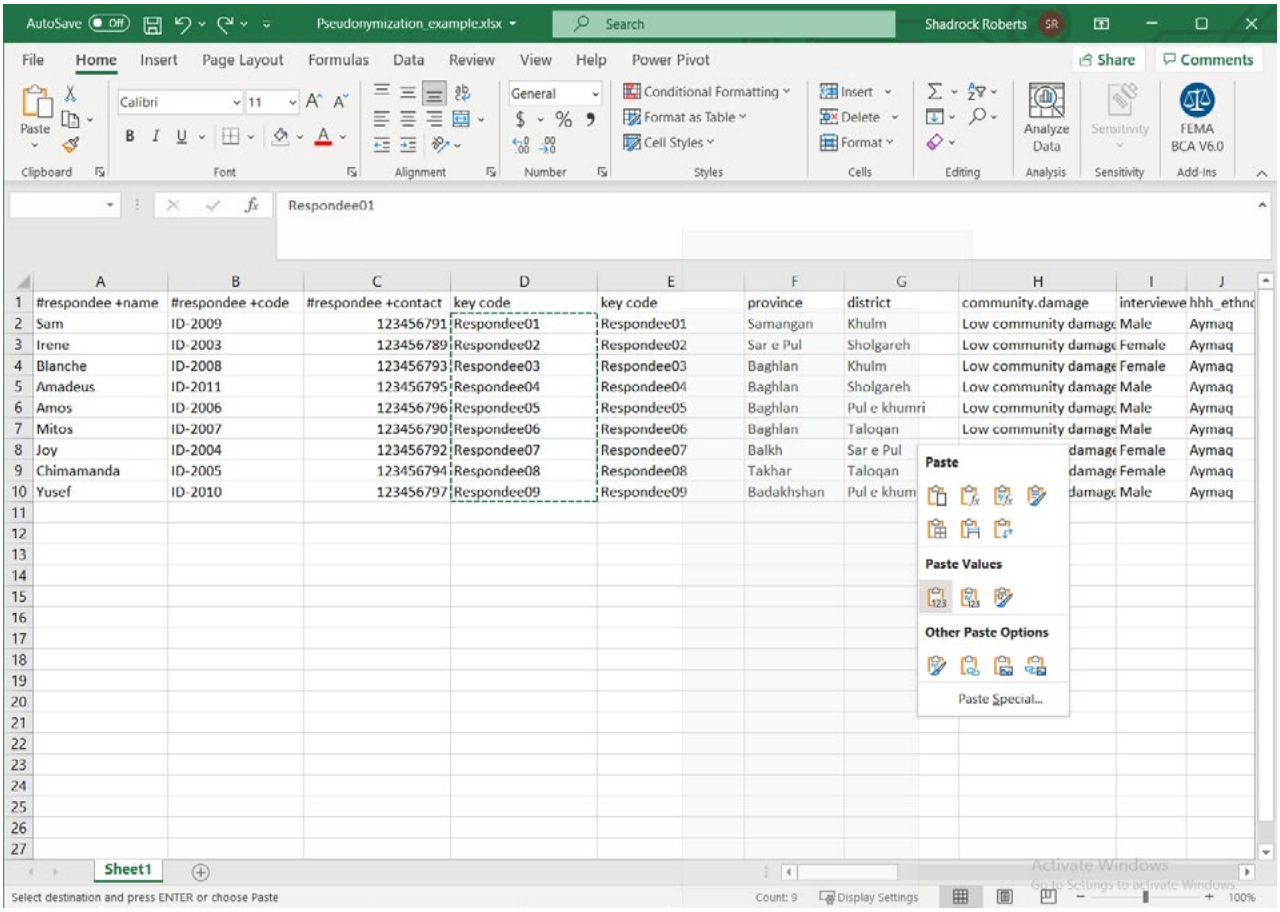
Paso 3: crear el código clave

Comience por nombrar sus nuevas columnas. Usaremos el «código clave» en cada una de ellas: cada columna contendrá los mismos valores. Este sería un buen momento para actualizar los metadatos de este conjunto de datos y explicar el significado del **código clave**. A continuación, usaremos la función de Llenado Automático de Excel para crear un código sencillo. Escriba **Respondee01** en la primera celda. A continuación, resalte esa celda, haga clic en el manejador de arrastre de la esquina inferior derecha de la celda y arrastre hasta el final del conjunto de datos. Esto llenará automáticamente el número final de cada registro para que cada respondedor tenga ahora un nuevo código.



Paso 4: duplicar el código clave y eliminar las fórmulas

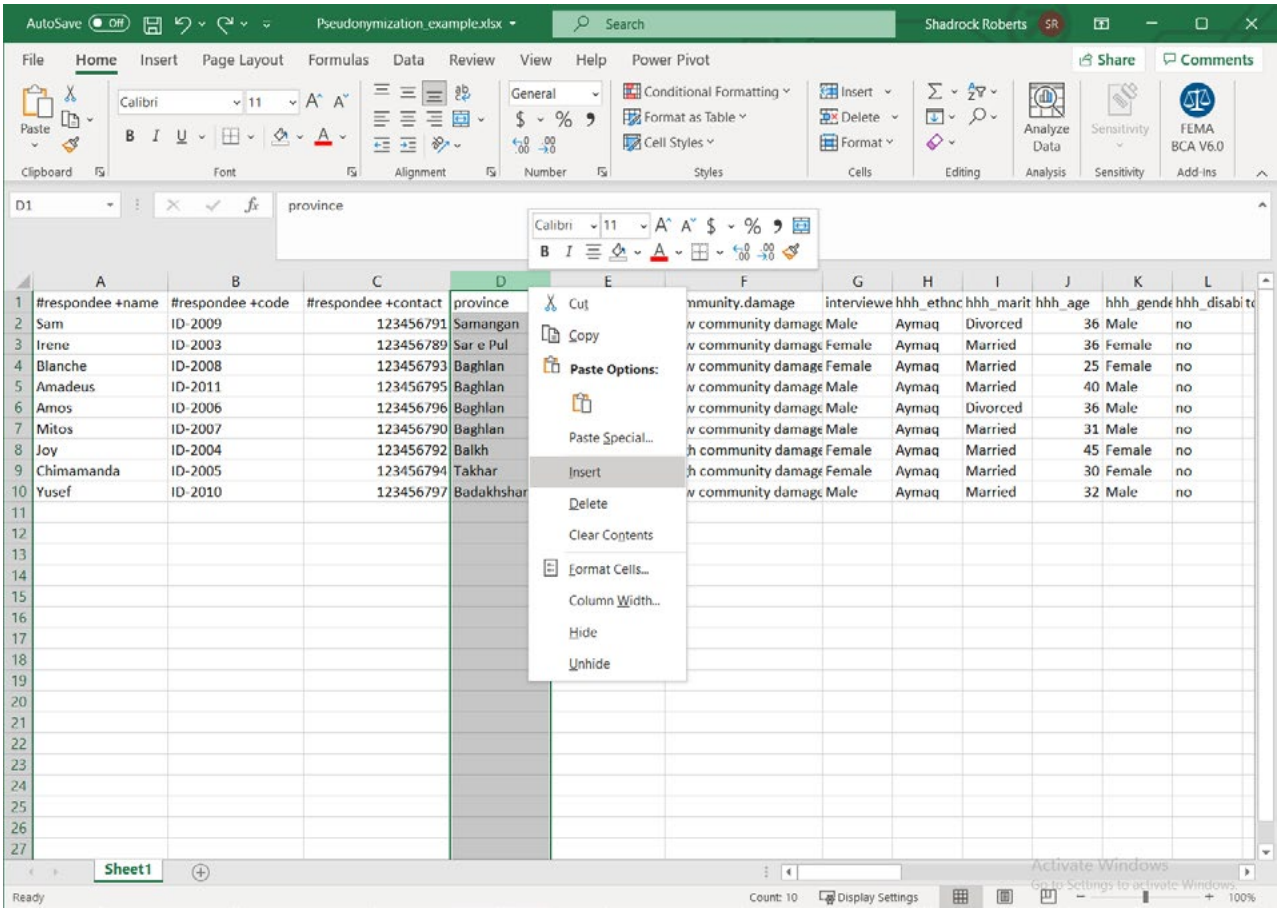
Ahora copiaremos el código clave y lo pegaremos en la columna adyacente. Puede hacerlo con comandos básicos del teclado como **ctrl + C** o al resaltar las celdas que desea copiar, al hacer clic con el botón derecho del mouse y seleccionar **Copiar**. En la columna adyacente, resalte las celdas en las que desea pegar el nuevo código clave, haga clic con el botón derecho y elija **Pegar**. Opté por pegar específicamente solo los valores. Si ha usado una fórmula para crear un nuevo código, ¡será importante conservar *solo los valores* para usarlos como código clave!



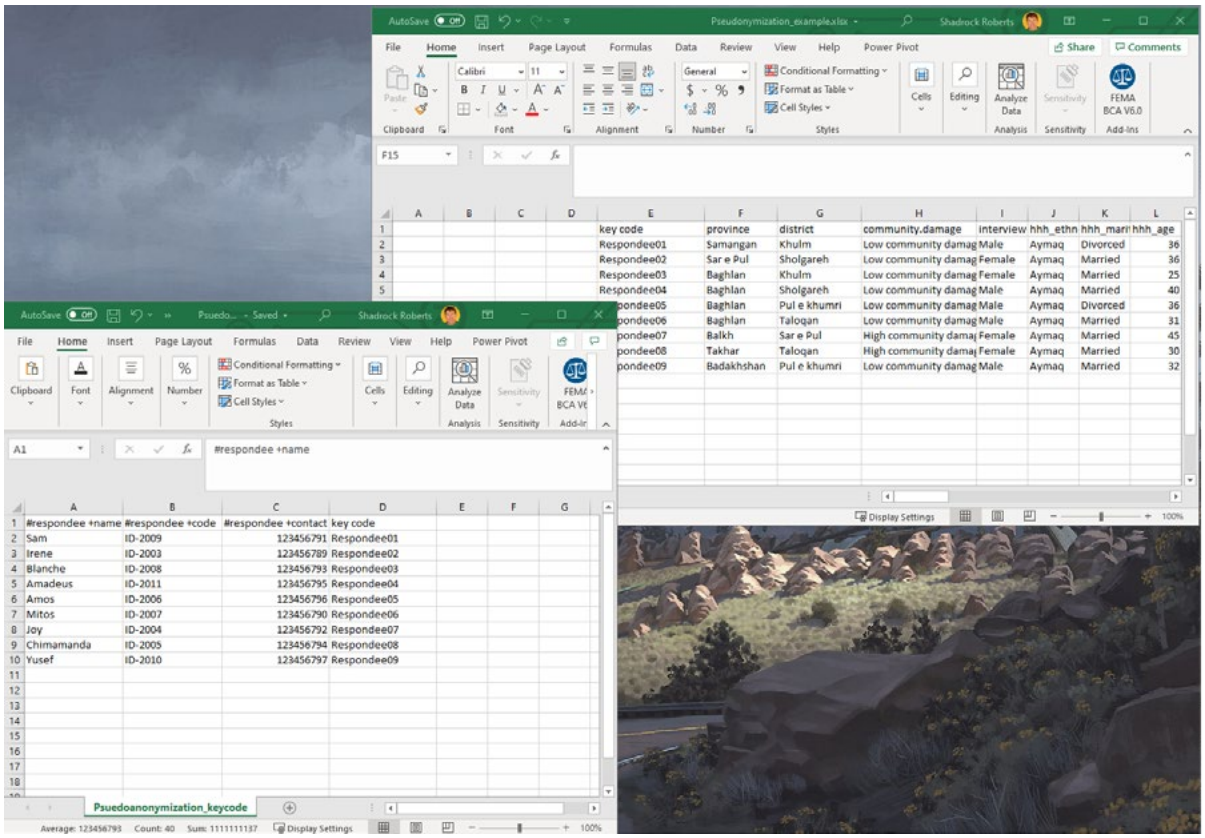
	A	B	C	D	E	F	G	H	I	J
1	#respondee +name	#respondee +code	#respondee +contact	key code	key code	province	district	community.damage	interviewe	hhh_ethnc
2	Sam	ID-2009	123456791	Respondee01	Respondee01	Samangan	Khulm	Low community damage	Male	Aymaq
3	Irene	ID-2003	123456789	Respondee02	Respondee02	Sar e Pul	Sholgareh	Low community damage	Female	Aymaq
4	Blanche	ID-2008	123456793	Respondee03	Respondee03	Baghlan	Khulm	Low community damage	Female	Aymaq
5	Amadeus	ID-2011	123456795	Respondee04	Respondee04	Baghlan	Sholgareh	Low community damage	Male	Aymaq
6	Amos	ID-2006	123456796	Respondee05	Respondee05	Baghlan	Pul e khumri	Low community damage	Male	Aymaq
7	Mitos	ID-2007	123456790	Respondee06	Respondee06	Baghlan	Taloqan	Low community damage	Male	Aymaq
8	Joy	ID-2004	123456792	Respondee07	Respondee07	Balkh	Sar e Pul	damage	Female	Aymaq
9	Chimamanda	ID-2005	123456794	Respondee08	Respondee08	Takhar	Taloqan	damage	Female	Aymaq
10	Yusef	ID-2010	123456797	Respondee09	Respondee09	Badakhshan	Pul e khum	damage	Male	Aymaq

Paso 5: separar los identificadores directos e indirectos

Resalte las columnas que tienen los identificadores directos con PII junto con una de las columnas de códigos clave. En este ejemplo, resaltamos las columnas A-D. Haga clic con el botón derecho sobre ellas y seleccione **Cortar**.



A continuación, abra una nueva hoja de cálculo y pegue estos valores con el atajo de teclado **ctrl + V**, u otro método. Guarde la nueva hoja de cálculo. Ahora tiene dos hojas de cálculo: una tiene los identificadores indirectos mientras que la nueva tiene los identificadores directos con PII. Ambos conjuntos de datos tienen un código clave para cada registro de los datos, de modo que todos los datos se puedan recombinar cuando sea necesario.



Próximos pasos

Ambos archivos tienen un código clave que permitirá volver a unirlos. Una forma de hacer esto en Excel, es usar la función VLOOKUP para llenar automáticamente las celdas según el valor de otras celdas. En este caso, podría llenar las celdas vacías del archivo original con la PII que falta, según el valor del **código clave**.

Dado que el nuevo archivo tiene los identificadores directos que tienen PII, se debe almacenar de forma segura. Una forma excelente de hacerlo es cifrar el archivo y usar el almacenamiento en la nube para limitar el acceso al archivo (**consulte las guías de buenas prácticas de cifrado y uso compartido de archivos**).

Recuerde: aunque se ha desidentificado la hoja de cálculo original al eliminar los identificadores directos que tienen PII evidentes, los demás identificadores indirectos tienen el potencial de combinarse con otros datos o analizarse de forma que permitan identificar a una persona.

Por esta razón, ambos archivos se deben seguir almacenando de forma segura. Si se desea compartir el archivo original, no-PII, de forma más amplia, sería fundamental realizar *una evaluación del riesgo de divulgación* para garantizar que el riesgo de que los datos puedan ser reidentificados sea mínimo. El Centro de Datos Humanitarios tiene un tutorial en línea para realizar una evaluación del riesgo de divulgación con el

software estadístico de código abierto «R». Además, la página web de Poverty Action Lab's De-identification for data publication (Desidentificación para la publicación de datos) ofrece un excelente debate sobre la desidentificación de datos e incluye un código de muestra para el software estadístico Stata. Para el personal de Mercy Corps, el borrador de la guía de T4D está disponible internamente y proporciona fórmulas adicionales en Excel.

Por último, todos estos pasos juntos ayudan a mitigar el riesgo o la exposición de la PII, por lo que deben estar en la PIA (**consulte la guía de Evaluación de impacto en la privacidad**) para que otros entiendan cómo se protegen estos datos.

Asistencia adicional

La desidentificación de los datos forma parte de las buenas prácticas de gestión de datos y del ciclo de vida más amplio de los datos, que son las actividades generales de recolección de datos individuales como parte de un programa o respuesta. Los siguientes recursos son excelentes para comenzar a comprender mejor la gestión de los datos de forma responsable.

- El conjunto de herramientas para la responsabilidad de los datos de Cash Learning Partnership está diseñado específicamente para los profesionales que reciben su pago en efectivo y vales, pero es una regla de oro en la orientación para los datos responsables. El conjunto de herramientas está disponible en inglés, árabe, francés, y español.
- El *conjunto de iniciación a los datos para el personal humanitario de campo de la Red de Aprendizaje sobre Transferencias Monetarias Electrónicas (Electronic Cash Transfer Learning Action Network)* ofrece una serie de hojas de consejos sobre datos para comprender diversos aspectos de las buenas prácticas de gestión y protección de datos.
- El *Manual de protección de datos en Acciones Humanitarias del Comité Internacional de la Cruz Roja* es una guía detallada de casi todos los aspectos de los datos humanitarios. El capítulo 2 trata específicamente sobre la desidentificación de los datos.
- El Engine Room's *Handbook of the Modern Development Specialist (Manual de la Sala de Máquinas del Especialista Moderno en Desarrollo)* es una buena visión general de los datos en el contexto de las actividades de desarrollo internacional. La sección sobre el *Intercambio de datos* trata específicamente de la desidentificación.

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.

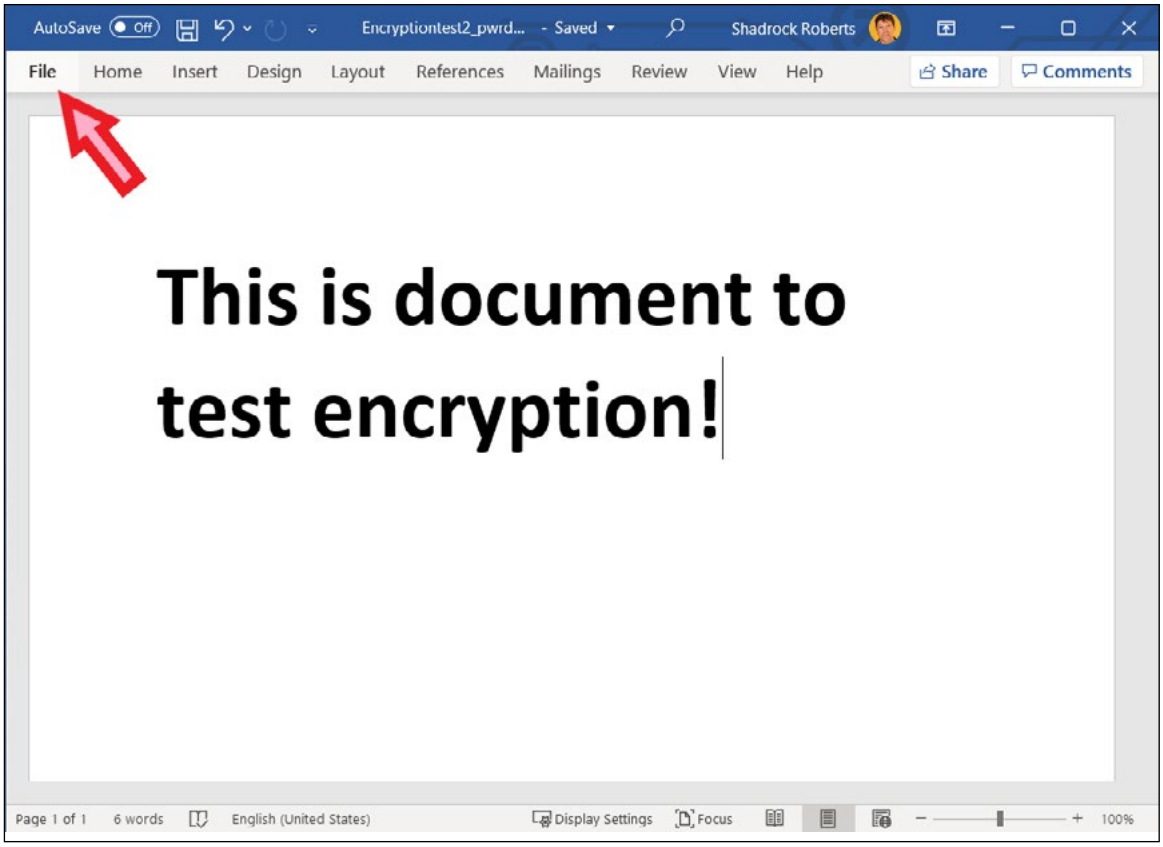
Principios

- 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.

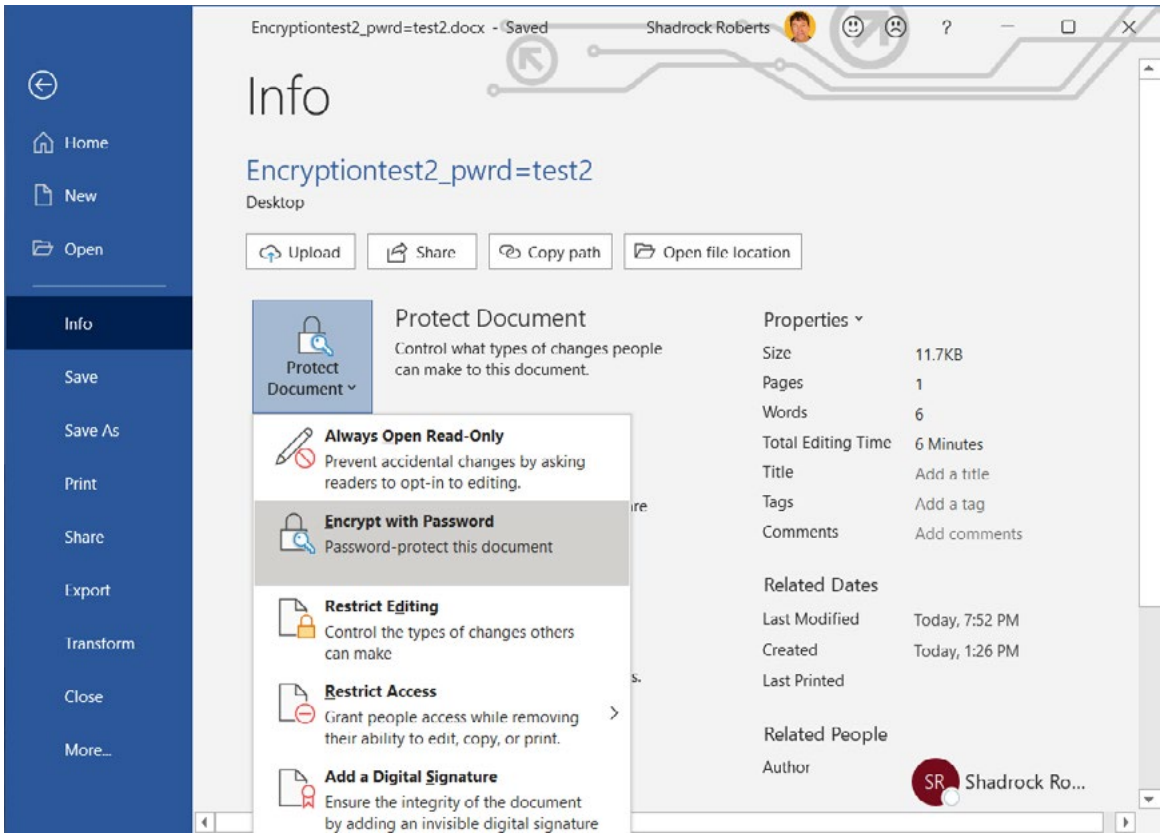
- En un entorno de equipo, el cifrado es tan bueno como el eslabón más débil. Si una sola persona no usa el cifrado, los datos del programa están en peligro. Comunicarlo a su equipo es extremadamente importante: el cifrado no es solo una cuestión de tecnología, sino también de cambio de comportamiento.
- 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

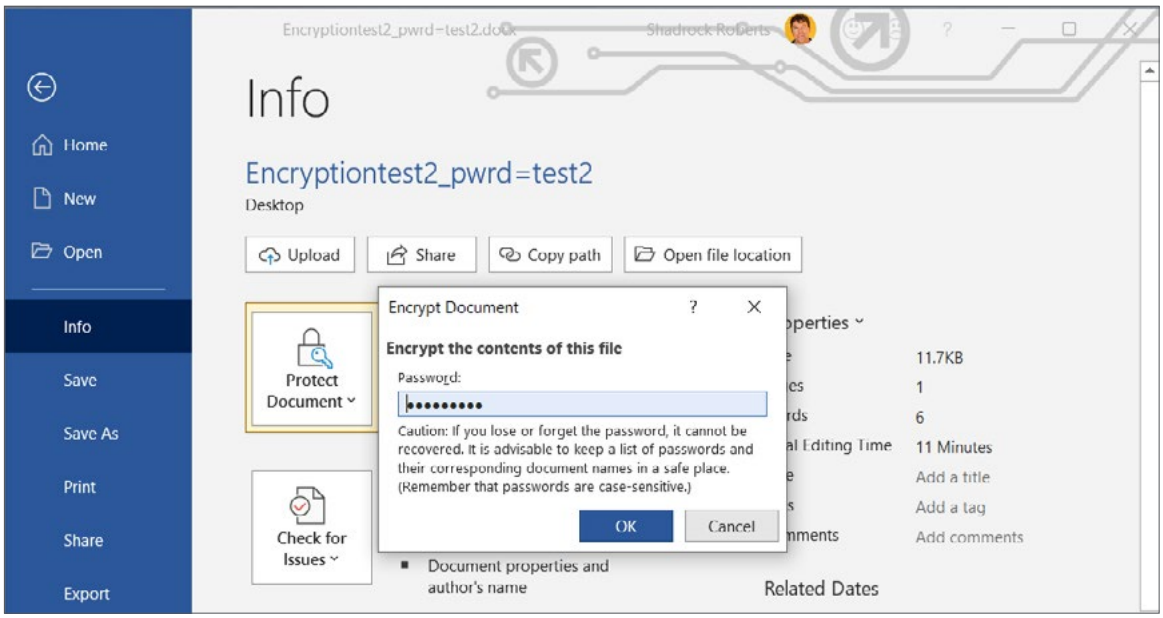
1 Abra el archivo de Word, Excel o PowerPoint que desea cifrar y seleccione el menú **Archivo**.



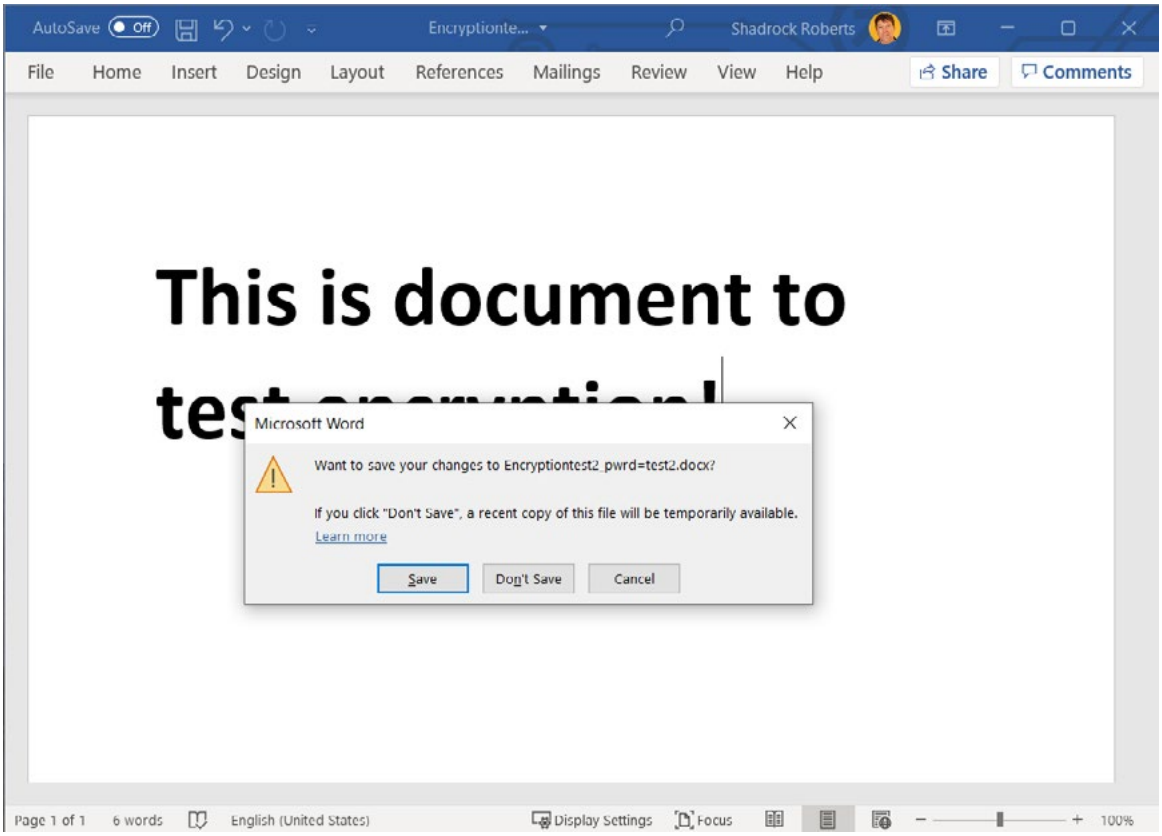
2 Desplácese a **Información** > **Proteger documento** > **Cifrar con contraseña**.



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