ALMACENAMIENTO Y TRANSFERENCIA ELECTRÓNICA DE DATOS PERSONALES DE PERSONAS DE INTERÉS FUERA DE PRIMES

Guía interna del ACNUR [febrero de 2021, versión 1]

Publicación conjunta del Oficial de Protección de Datos (Servicio Global de Datos, GDS, por sus siglas en inglés) y del Oficial Principal de Seguridad de la Información (División de Sistemas de Información y Telecomunicaciones, DIST, por sus siglas en inglés), en colaboración con la División de Protección Internacional (DIP, por sus siglas en inglés), la Sección de Asuntos Jurídicos (LAS, por sus siglas en inglés) y la Sección de Registros y Archivos (RAS, por sus siglas en inglés).

Antecedentes

En ACNUR, la gran mayoría de los datos personales de las personas de interés (PoC, por sus siglas en inglés) se almacenan y procesan actualmente en las herramientas del Ecosistema de registro y gestión de la identidad de la población (PRIMES [1]). Las herramientas PRIMES están diseñadas específicamente para ACNUR y ofrecen una serie de características de seguridad de los datos. Sin embargo, no todos los datos personales de las PoC pueden almacenarse o transferirse a través de PRIMES. El almacenamiento y la transferencia de datos personales de PoC fuera de PRIMES pueden ser necesarios, por ejemplo, para la gestión de casos fuera de línea que no está contemplada en la herramienta "RApp", o para otra recopilación de datos, evaluación de necesidades y/o monitoreo. También puede ser necesario el uso de herramientas ajenas a PRIMES para la comunicación bidireccional entre ACNUR y las PoC, utilizando herramientas y aplicaciones disponibles para las PoC.

[1] *Para más información sobre PRIMES, consulte: https://www.acnur.org/registro.html?query=registro%20y%20gesti%C3%B3n%20de%20identidad .*

1. Objetivo y destinatarios

1.1 El objetivo de esta Guía Interna es informar a todo el personal de ACNUR sobre cómo cumplir con la Política sobre la Protección de Datos[2] (DPP, por sus siglas en inglés) de ACNUR cuando se utiliza o se considera el uso de herramientas y aplicaciones fuera de PRIMES para almacenar y transferir electrónicamente los datos personales de las PoC. Tiene en cuenta las instrucciones y directrices aplicables emitidas por la DIST y se basa en la Guía sobre la Protección de Datos[3] (DPG, por sus siglas en inglés).

1.2 Esta guía interna ha sido elaborada conjuntamente[4] por el Oficial de Protección de Datos (DPO) del ACNUR, el Oficial Principal de Seguridad de la Información (CISO, por sus siglas en inglés) y en colaboración con la DIP, LAS y RAS. No puede ni pretende establecer nuevas normas. Más bien, proporciona asesoría detallada y actualizada sobre una serie de herramientas para el almacenamiento y la transferencia de los datos personales de las PoC, y su nivel requerido de seguridad de los datos.

2. Fundamento

2.1 El ACNUR en el ejercicio de su mandato de proporcionar protección internacional y soluciones a los refugiados, a menudo es necesario que este organismo procese los datos personales de las personas de interés.[5] El almacenamiento y la transferencia de datos personales son dos tipos importantes de tratamiento de datos.[6] Ya sea que los datos estén en reposo o en tránsito[7], es fundamental garantizar un alto nivel de seguridad de los datos y prevenir las filtraciones de los datos personales.[8]

2.2 En ACNUR, la gran mayoría de los datos personales de las PoC se almacenan y procesan actualmente en las herramientas PRIMES, principalmente proGres v4, el Sistema de Gestión de Identidad Biométrica (BIMS), la Aplicación Rápida (RApp), CashAssist y/o la Herramienta de Distribución Global (GDT). Las herramientas PRIMES están diseñadas específicamente para ACNUR y ofrecen una serie de características de seguridad de los datos. Todas las herramientas principales de PRIMES se están

[2] *ACNUR,* Política sobre la Protección de Datos Personales de las Personas de Interés del ACNUR (DPP), ***HCP/2015/6,*** *mayo de 2015, disponible en:* ***https://www.refworld.org.es/docid/5d7fd103a.html****..*

[3] *ACNUR,* Guía sobre la protección de datos personales de las personas de interés del ACNUR (DPG), *agosto de 2018, disponible en inglés en: https://www.refworld.org/docid/5b360f4d4.html.*

[4] *Dentro de las atribuciones del Oficial de Protección de Datos, según el apartado. 7.3 de la DPP.*

[5] *ACNUR,* Política de protección de datos personales de las personas de interés del ACNUR (DPP), ***HCP/2015/6,*** *mayo de 2015, disponible en: https://www.refworld.org.es/docid/5d7fd103a.html,* ***párr. 1.2.1.***

[6] *Véase el párrafo 1.4 de la DPP para la definición de "tratamiento de datos personales": "Cualquier operación o conjunto de operaciones, automatizadas o no, que se realiza en relación a los datos personales, incluyendo pero no limitado a la recopilación, registro, organización, estructuración, almacenamiento, adaptación o modificación, recuperación, consulta, uso, transferencia (ya sea en forma computarizada, oral o escrita), difusión o cualquier otra puesta a disposición, corrección o destrucción".*

[7] *Véanse en las secciones pertinentes de esta nota interna las definiciones de datos en tránsito (sección 8) y datos en reposo (sección 5).*

[8] *Véase el párrafo 1.4 de la DPP para la definición de "filtración de datos personales". "Una violación de la seguridad de los datos que conduce a la destrucción, perdida, alteración, divulgación no autorizada o acceso accidental o ilegal/ilícita de datos personales transferidos, almacenados o de otro modo procesados".*

sometiendo o se han sometido ya a una Evaluación de Impacto de la Protección de Datos (DPIA, por sus siglas en inglés).[9] A través del acceso al perfil de socio de proGres v4, las herramientas PRIMES también permiten la transferencia de datos personales de las PoC a socios preautorizados mediante la concesión de acceso a la plataforma.

2.3 Sin embargo, no todos los datos personales de las PoC pueden almacenarse o transferirse a través de PRIMES. El almacenamiento y la transferencia de los datos personales de las PoC fuera de PRIMES pueden ser necesarios para la gestión de casos fuera de línea que no son atendidos por RApp, o para otra recopilación de datos, evaluación de necesidades y/o monitoreo. También puede ser necesario el uso de herramientas ajenas a PRIMES para la comunicación bidireccional entre ACNUR y las PoC, utilizando herramientas y aplicaciones que están a disposición de las PoC.

3. Alcance y estructura

3.1 Esta Guía Interna cubre los temas de todo el almacenamiento electrónico y la transferencia de datos personales de las PoC fuera de PRIMES. La orientación sustantiva se presenta en las cinco secciones siguientes: La sección 4 resume la política y la guía existentes relacionadas con el almacenamiento y la transferencia de datos; la sección 5 describe los requisitos para el almacenamiento seguro de los datos personales de las PoC en general (datos "en reposo"); las secciones 6 y 7 examinan más específicamente el almacenamiento en línea y fuera de línea; y la sección 8 trata de la comunicación y la transferencia seguras de datos (datos "en tránsito").

4. Requisitos de políticas y guías existentes sobre la seguridad de los datos

4.1 Política sobre la protección de datos del ACNUR (DPP) [10]y Política de clasificación, manejo y divulgación de la información del ACNUR ("Política de clasificación de la información"). [11]

4.1.1 La seguridad de los datos personales es un principio fundamental de la DPP del ACNUR (párr. 2.1 (vii) y 2.8). El párr. 4.2 de la DPP, la principal disposición sobre la seguridad de los datos incluye una serie de afirmaciones:

1) la necesidad de "garantizar e implementar un alto nivel de seguridad de los datos que se adecue a los riesgos que entraña la naturaleza y el procesamiento de los

[9] *Véase el párrafo 4.5 de la DPP y la sección 8 de la DPG. 4.5 y la sección 8 de la DPG para más detalles sobre las DPIA.*

[10] *ACNUR,* Política de protección de datos personales de las personas de interés del ACNUR (DPP), *HCP/2015/6, mayo de 2015, disponible en: https://www.refworld.org.es/docid/5d7fd103a.html.*.

[11] *ACNUR,* Política de clasificación, manejo y divulgación de la información del ACNUR, *IOM/076-FOM/076/2010, 2010, disponible en inglés en: https://intranet.unhcr.org/en/policy-guidance/iomfoms/iom-076-fom-076-2010.html*

.

datos personales, la disponibilidad y la calidad de los equipos necesarios, el costo y la viabilidad operativa" (párrafo 4.2.1).

2) la necesidad de "poner en práctica medidas organizativas y técnicas adecuadas para garantizar que el procesamiento cumpla con los requisitos de la presente Política. Esto incluye la implementación de tecnologías para mejorar la protección de datos y herramientas que permitan a los procesadores de datos mejorar la protección de los datos personales ("privacidad por diseño y por defecto")" (párrafo 4.2.3).

3) Entre las medidas técnicas, el DPP identifica "el mantenimiento de la seguridad del equipo y la tecnología de la información (IT, por sus siglas en inglés), por ejemplo, el control de acceso (por ejemplo, contraseñas, acceso por niveles), control de usuario, control de almacenamiento, control de entrada, control de comunicación y transporte (por ejemplo, la encriptación)" (4.2.5 (ii)).

4.1.2 El principio de confidencialidad está estrechamente relacionado con el principio de seguridad de los datos personales (DPP 2.7). Según el párr. 4.1.1, los datos personales de las PoC están clasificados por definición como confidenciales, y su confidencialidad debe ser respetada por ACNUR al procesarlos en todo momento.

4.1.2 La Política de Clasificación de la Información del ACNUR exige que la transmisión electrónica de toda la información clasificada se realice únicamente mediante el uso de medios de comunicación protegidos y que todos los datos clasificados se archiven y almacenen de manera que sólo sean accesibles para los funcionarios autorizados (párrafo V. 1). Por lo que respecta a los sistemas de información automatizados utilizados para la recolección, tratamiento y transferencia de información clasificada, la Política de Clasificación de la Información exige además que dichos sistemas "dispongan de controles que impidan el acceso de personas no autorizadas y garanticen la integridad de la información" (traducción libre) (párrafo V.3).

4.2 Guía sobre la Protección de Datos[12] (DPG)

4.2.1 A efectos del almacenamiento y la transferencia electrónicos de los datos personales de las PoC, la asesoría proporcionada en la DPG ya no puede considerarse exhaustiva ni actualizada. Por ejemplo, asesora utilizar únicamente "herramientas corporativas del ACNUR" o "herramientas desarrolladas y aprobadas por el ACNUR" (párr. 6.3.7 (i) y 6.6.2 (i)), lo que no está claramente definido y no siempre es posible. En cuanto al almacenamiento, recomienda a "las oficinas con acceso confiable a Internet que almacenen expedientes electrónicos en e-SAFE; las oficinas sin dicho acceso deben establecer una unidad compartida restringida. Los datos personales de las personas de interés no se deben almacenar en las unidades de red personales*" (párrafo* 6.3.7 (iii) de la DPG). Aunque esto sigue siendo esencialmente válido, la pandemia de COVID-19 ha acentuado la necesidad de acceso remoto en línea, que no puede ser soportado por las

[12] *ACNUR,* Guía sobre la protección de datos personales de las personas de interés del ACNUR (DPG), *agosto de 2018, disponible en inglés en: https://www.refworld.org/docid/5b360f4d4.html.*

redes de área local (LAN, es decir, unidades compartidas restringidas), y ha acelerado el uso de las funciones de almacenamiento y de compartir datos en línea de Office 365, como Teams y SharePoint. [13]

4.2.2 Con respecto a las comunicaciones y transferencias de datos seguras, la DPG (Sección 6.6) establece lo siguiente:

- Ninguna información de carácter confidencial debe ser enviada por correo electrónico a través de Internet (que incluye los datos de las PoC),
- los datos personales no deben ser transferidos usando cuentas de correo electrónico personales o a través de cuentas de redes sociales,
- y los SMS deben evitarse como medio para comunicar datos personales.[14]

4.2.3 La DPG también identifican alternativas más seguras al correo electrónico a través de Internet, incluyendo el uso de e-SAFE, los servicios de protocolo de transferencia segura de archivos (SFTP, por sus siglas en inglés) del ACNUR y los dispositivos de medios portátiles encriptados (párrafo 6.6.2 (iii)). Si se usa el correo electrónico, asegurarse de que se tomen medidas adicionales para proteger el contenido, como el cifrado del correo electrónico o su archivo adjunto, e indica que los servicios de mensajería de texto que están cifrados de extremo a extremo son más seguros que los mensajes SMS y deberían utilizarse en su lugar (párrafo 6.6.2 (v) y (vi)). Sin embargo, la DPG no aborda el uso de canales de mensajería (WhatsApp, Signal, WeChat), ni de herramientas de conferencia (Microsoft (MS) Teams, WebEx, Skype, Zoom, etc.). Tampoco tiene en cuenta el servicio de Intercambio Seguro de Archivos (SFS, por sus siglas en inglés) de ACNUR, que no estuvo disponible hasta agosto de 2019 (es decir, un año después de la publicación de la DPG).

4.2.4 Además, la DPG no aborda la necesidad de una identificación adecuada y fiable del personal cuando accede a los datos personales de las PoC. En la actualidad, esto se lleva a cabo generalmente a través de la autenticación de dos factores o multifactor (MFA, por sus siglas en inglés), que se basa en "algo que se tiene" (por ejemplo, un teléfono móvil) y "algo que se sabe" (la contraseña). La MFA se ha vuelto indispensable como medida de seguridad con la creciente necesidad de acceso y tratamiento de datos a distancia. [15]

---

[13] *Véase, ACNUR,* "Office 365: Collaboration and communications tools that help you save time, costs and hassles in delivering to those we serve" (Office 365: Herramientas de colaboración y comunicación que le ayudan a ahorrar tiempo, costos y molestias en la prestación de servicios a las personas que servimos), *disponible en inglés en: https://intranet.unhcr.org/en/support-services/ict-operations/ict-services/software_business_applications/microsoft-office-365.html.*

[14] *Véase el parágrafo. 6.6.2 (iii), (iv) y (vi) de la DPG. Paréntesis añadidos.*

[15] *Véase ACNUR,* Protecting your account with Multi-Factor Authentication (Protección de su cuenta con autenticación multifactor), *enero de 2020, disponible en inglés en: https://intranet.unhcr.org/en/support-services/ict-operations/ict-services/accounts-passwords/introducing-multi-factor-authentication-.html.*

5. Almacenamiento electrónico seguro (datos "en reposo")

Esta sección describe los requisitos y la asesoría para el almacenamiento seguro de los datos personales de las PoC fuera de PRIMES.

5.1 Preferencia por las herramientas corporativas

5.1.1 La recomendación del párrafo. 6.3.7 (i) de la DPG de "que solo utilicen herramientas corporativas de ACNUR" debería completarse y aclararse en el sentido de que se recomienda a las operaciones que eviten almacenar los datos personales de las PoC fuera de PRIMES en la medida en que sea razonablemente posible. Cuando los datos personales de las PoC **deban** almacenarse fuera de PRIMES, las herramientas corporativas del ACNUR deben tener prioridad sobre las herramientas no corporativas. Las herramientas corporativas incluyen no solo PRIMES, sino también e-SAFE y las herramientas de Office 365 Suite, concretamente MS Teams y SharePoint [16].

5.1.2 El almacenamiento de datos personales de las PoC fuera de PRIMES puede, no obstante, estar justificado. La decisión debe basarse en una determinación de las necesidades por escrito y en la recopilación de los requisitos de los productos y servicios, cuando proceda realizar una evaluación de riesgos y/o una DPIA, y la solución seleccionada debe ofrecer garantías equivalentes a los datos personales de las PoC, incluidos los requisitos expresados a continuación.

5.1.3 En lo que respecta a la adquisición de equipos y servicios TI, deberán observarse las orientaciones contenidas en las Directrices operativas de presupuesto y adquisición de equipos y servicios de TI. [17]

5.1.4 En el apartado 4.4.3 de estas directrices se indica que "Antes de adquirir software de uso local, la oficina debe coordinar con DIST (TI en Operaciones de campo) y DESS (Servicio de adquisiciones) para ver si ya existe alguna licencia global y/o si los beneficios de adquirir localmente superan con creces el uso de acuerdos de licencia global", [18] (traducción libre).

5.1.5 Una solución estándar de ACNUR, por lo general, ya habrá garantizado los privilegios e inmunidades de las Naciones Unidas en relación con el almacenamiento y el tratamiento de los datos personales de las PoC en la medida en que tenga lugar en los servidores y servicios del proveedor de servicios con el que ACNUR tiene un acuerdo contractual.

---

[16] *Una herramienta corporativa desarrollada por ACNUR, alojada en servidores seguros, utiliza MFA, etc.*

[17] *ACNUR, ,* Operational Guidelines for Budgeting and Procurement of ICT equipment and services (Directrices operativas de presupuesto y adquisición de equipos y servicios de TIC) (UNHCR/OG/2015/6/Rev.2), abril de 2017, *disponible en inglés en: https://intranet.unhcr.org/en/policy-guidance/operational-guidelines/unhcr-og-2015-6-rev-2.html.*

[18] *Ídem.*

5.1.6 En las situaciones en las que las soluciones estándar de ACNUR no satisfacen los requisitos y se encargan nuevos servicios, es responsabilidad del controlador de datos de ACNUR que requiera una solución alternativa para garantizar que, si los datos personales de las PoC van a ser almacenados y/o tratadas por un proveedor, se respeten los requisitos del capítulo 6 de la DPP relativos a la transferencia de datos personales a un tercero. Estos requisitos incluyen la salvaguarda de los privilegios e inmunidades del ACNUR y la revisión y autorización del contrato propuesto con el proveedor por parte del Servicio de Asuntos Jurídicos (LAS) y el DPO. [19]

5.2 Encriptación

5.2.1 Cuando una operación de un país o una entidad regional o de la sede pretenda almacenar datos personales de las PoC fuera de PRIMES, los datos personales deberán estar **encriptados,** es decir, almacenados en unidades encriptadas o con servicios de terceros que utilicen un algoritmo[20] de encriptación eficaz[21].

5.2.2 Para los ordenadores y servidores Windows del ACNUR, el único sistema de cifrado corporativo, y muy recomendado, es BitLocker. Se trata de la herramienta estándar de Microsoft Windows para cifrar los discos duros y se está implantando en todos los ordenadores del ACNUR que lo soportan. BitLocker protege los datos almacenados en el disco duro de un ordenador (almacenamiento) contra la extracción por parte de un hacker o alguien con acceso físico no autorizado a la máquina. [22]

5.3 Autenticación multifactor

5.3.1 Las operaciones en los países y las entidades regionales y de la sede deben permitir el acceso a los datos personales de las PoC solo a los usuarios que tengan aplicada **la autenticación multifactor** (MFA) [23] en su cuenta.

5.3.2 La MFA ayuda a prevenir el riesgo de acceso no autorizado a los datos personales de las PoC en caso de que se comprometa una única contraseña a través de Internet, al requerir un token físico (teléfono, tarjeta, etc.) además de la contraseña.[24] En la Intranet del ACNUR se puede encontrar información sobre cómo instalar la MFA para las cuentas

---

[19] Véase el capítulo 6 y la sección 6.5 de la DPP.

[20] El encriptado es el procedimiento que convierte el texto claro en un código cifrado mediante una clave, donde la información saliente sólo vuelve a ser legible en el otro extremo utilizando la clave correcta. Véase, por ejemplo, Intersoft Consulting, GDPR: Key Issues - Encryption*, disponible en inglés en: https://gdpr-info.eu/issues/encryption/.*

[21] DIST publicará de vez en cuando directrices sobre los algoritmos de encriptado adecuados que deben utilizarse.

[22] ACNUR, Cifrado de disco BitLocker: Instalación y uso de la herramienta*, octubre de 2019, disponible en inglés en: https://intranet.unhcr.org/en/support-services/ict-operations/dist-faq-search/bitlocker-disk-encryption--installing-and-using-the-tool.html.*

[23] MFA se refiere al uso de dos métodos diferentes para identificarse, basados en "algo que se tiene" (por ejemplo, un teléfono móvil) y "algo que se sabe" (la contraseña).

[24] El acceso no autorizado a los datos personales de los PoC constituye una filtración de los datos personales y debe notificarse al Controlador de Datos y, si es probable que la filtración provoque daños personales o daños a un interesado, también al DPO (véase el apartado 4.4 de la DPP y la definición de filtración de los datos personales en el apartado 4.3 de la DPP).

de usuario. [25] Para obtener más recomendaciones sobre la MFA para aplicaciones no corporativas, se debe consultar al punto focal de TI de la operación del país, al jefe de TI del Buró regional o al oficial principal de seguridad de la información (CISO).

6. Almacenamiento en línea

6.1 Plataformas oficiales de almacenamiento

6.1.1 Las operaciones en los países y las entidades regionales y de la sede deben utilizar únicamente plataformas corporativas en línea. Las plataformas en línea oficiales (de ACNUR) para el almacenamiento de datos personales de las PoC incluyen e-SAFE, SharePoint, Microsoft Teams, Office 365 Forms y el servicio KoBo utilizado por ACNUR[26].

6.2 e-SAFE

6.2.1 e-SAFE es el sistema oficial de gestión de registros electrónicos de ACNUR.[27] Aunque e-SAFE no es un servicio PRIMES y todavía no ofrece un cifrado universal obligatorio, la MFA se implementó desde noviembre de 2020. e-SAFE se considera, por tanto, una plataforma aceptable con veinte años de práctica que implementa procedimientos claros de gestión de acceso estandarizados y estructuras de carpetas por niveles para permitir el acceso restringido a carpetas específicas en e-SAFE solo al personal autorizado[28] .

6.3 Plataformas de almacenamiento de datos en Office 365

6.3.1 Microsoft Office 365 incluye Microsoft Teams, SharePoint, Excel, Word, PowerPoint, OneDrive y otras herramientas. Específicamente para el almacenamiento de datos compartidos, MS Teams y SharePoint son las plataformas clave para el almacenamiento compartido y el co-working. El almacenamiento central en la "nube" (gestionado por Microsoft) que ofrecen está cifrado, al igual que el almacenamiento ofrecido en la nube en la carpeta personal de cada usuario en OneDrive (que se sincroniza con el ordenador del usuario). Tanto OneDrive como MS Teams y SharePoint utilizan el servicio global MFA (si está configurado para el usuario). El uso de los servicios de Microsoft por parte del ACNUR está protegido por cláusulas de privilegios e inmunidades en acuerdos vinculantes.

---

[25] *Véase ACNUR,* Protecting your account with Multi-Factor Authentication (Proteger su cuenta con la autenticación multifactor), *enero de 2020, disponible en inglés en: https://intranet.unhcr.org/en/support-services/ict-operations/ict-services/accounts-passwords/introducing-multi-factor-authentication-.html.*

[26] *Véase en inglés: https://intranet.unhcr.org/en/support-services/ict-operations/ict-services/collaboration/teams.html, https://intranet.unhcr.org/en/support-services/ict-operations/ict-services/collaboration/sharepoint-online.html y*

[27] *ACNUR,* ¿Qué es e-SAFE y por qué debería utilizarlo? *, mayo de 2018, disponible en inglés en: https://intranet.unhcr.org/en/support-services/RAS/ras-faqs/what-is-e-safe-and-why-should-i-use-it-.html.*

[28] *La Sección de Registros y Archivos de la División de Relaciones Exteriores ofrece orientación, apoyo y auditorías periódicas para la implementación del acceso.*

6.3.2 El personal del ACNUR no debe compartir la información de las PoC en ningún grupo de MS Teams o SharePoint ni a través de enlaces de archivos de Word a su OneDrive personal, a menos que se haya confirmado que todos los usuarios del "equipo" tienen nuestra identidad común del ACNUR (Office 365) MFA. Dado que la MFA aún no se aplica a todos los usuarios de ACNUR Office 365, el administrador del espacio compartido tendría que verificar que solo el personal de ACNUR con MFA sea admitido en ese espacio o se le envíen dichos enlaces.

6.3.3 Cuando se comparten archivos de datos de PoC en SharePoint Online hay tres opciones: "Personas en ACNUR con el enlace", "Personas con acceso existente" y "Personas específicas". Sólo debe utilizarse "Personas específicas" (de lo contrario, los archivos pueden ser accesibles para todo el personal de ACNUR).

6.3.4 El personal de ACNUR no debe almacenar las copias únicas o maestras de los datos de las PoC en OneDrive, ya que la cuenta se eliminará junto con toda su información una vez que ese miembro del personal se separe de ACNUR.

6.4 Redes de área local (LAN)

6.4.1 Las unidades compartidas de LAN de ACNUR, es decir, las unidades K:\ y L:\, no son un servicio PRIMES. Por lo general, no están encriptadas y no admiten la identidad común MFA. No se consideran una solución de almacenamiento de documentos a largo plazo para los datos personales de las PoC.[29] Sin embargo, hoy en día se utilizan ampliamente para ese propósito.

6.4.2 Las redes LAN están limitadas (físicamente) a una oficina y requieren algo que el usuario tenga (es decir, la presencia física del usuario) para acceder, o el uso de una solución de Red Privada Virtual (VPN), que normalmente requiere un certificado digital especial en el ordenador del usuario.[30] Por lo tanto, suele ser posible un nivel básico de autenticación multifactor.

6.4.3 Para mejorar la seguridad, el uso de las unidades LAN que contengan datos personales de las PoC debe limitarse siempre a los usuarios autorizados nombrados, sobre la base de la "necesidad de saber" (según los principios de la DPP de finalidad, necesidad y confidencialidad), y protegidos por contraseña.

6.5 KoBo (software hosted por ACNUR)

6.5.1 La caja de herramientas KoBo es un conjunto de herramientas de código abierto para la recopilación y el análisis de datos en emergencias humanitarias mediante

[29] *Véase Sección de Registros y Archivos del ACNUR,* Guidance on how to share and organize information*, Records and Archives Management Guidance (Directrices sobre cómo compartir y organizar información, Registros y Directrices para la gestión de archivos.): RAS/RM/EXT/28-00/v1, última actualización 10 nov 2020, y DIST,* Guidelines for Migrating Network (J:, L: and K:) Drives*, abril 2020, versión 1.0, disponible en inglés en: https://intranet.unhcr.org/content/dam/unhcr/intranet/staff%20support/information-communication-technology/documents/english/office365/Guidelines%20for%20Migrating%20Network%20Drives.pdf*

[30] *Una VPN es un servicio que crea una conexión encriptada entre un servidor VPN y el propio dispositivo. Véase Cybersecurity Insiders,* How VPNs Keep Your Data Secure, *disponible en inglés en: https://www.cybersecurity-insiders.com/how-vpns-keep-your-data-secure/.*

dispositivos móviles como teléfonos móviles, tabletas u ordenadores.[31]ACNUR ofrece su propia instancia de KoBo, que está vinculada al servicio en la nube de Amazon Web Services (AWS) de ACNUR y cuenta con el apoyo del equipo técnico de ACNUR. KoBo está diseñado principalmente para facilitar la recopilación digital de datos primarios y su posterior análisis. Con el traslado del servidor KoBo de ACNUR a AWS, todos los datos almacenados están encriptados en reposo y en una plataforma que respeta los privilegios e inmunidades de ACNUR.

6.5.2 Como sistema de código abierto, el acceso y el uso de KoBo se basa en el auto registro. Cualquier usuario, incluso personas ajenas al ACNUR, puede registrarse para abrir una cuenta de KoBo del ACNUR. Existe un panel de gestión de usuarios centralizado en el que el equipo de KoBo de la sede puede acceder a todas las cuentas de usuario. Sin embargo, no existe el mismo acceso para proyectos específicos: el KoBo de la sede "encarnará" a un usuario para obtener acceso a sus proyectos o tener acceso a un proyecto específico a través de "compartir". Actualmente, esto se hace después de que el propietario del proyecto haya concedido el permiso a través de un perfil de usuario conocido como "gestión de proyectos". En vista de su sencillo modelo de seguridad, y de la falta de MFA y de supervisión centralizada sobre el uso (aún se espera que se complete a finales de 2021), el tratamiento de los datos personales de las PoC en KoBo de ACNUR está permitido, pero debe ser cuidadosamente controlado por el propietario del proyecto, en estrecha coordinación con el equipo de KoBo de la sede. La caja de herramientas de KoBo debe utilizarse como herramienta principal de recolección de datos y, una vez recogidos, deben trasladarse a otra plataforma para su almacenamiento[32].

6.5.3 Para ello, se recomienda que las operaciones de países consideren el uso de las funcionalidades de integración de KoBo en proGres v4. Esta función sólo crea un enlace entre un formulario KoBo y un registro en proGres v4 (por ejemplo, un registro individual o un registro de grupo), mientras que los datos se almacenan en los respectivos servidores (es decir, el servidor KoBo AWS de ACNUR y el servidor proGres de ACNUR en Safe Host). De este modo, las operaciones pueden garantizar mejor que los datos personales de las PoC se almacenen de forma segura en PRIMES, mientras que los datos no personales se almacenan en KoBo. Para obtener más asesoría sobre la mejora de la seguridad (por ejemplo, sobre el encriptado de los formularios de KoBo), los usuarios de KoBo de ACNUR deben ponerse en contacto con el Servicio Global de Datos para enviar solicitudes de asistencia. El equipo de soporte de KoBo de la GDS puede ponerse en copia de la solicitud en kobohq@unhcr.org

6.6 Otras plataformas de almacenamiento

6.6.1 Otras plataformas de almacenamiento, incluidas las soluciones gratuitas en línea, como Dropbox, Boot Camp, Apple iCloud, Google Drive y Forms, registradas personalmente, **no deben** utilizarse nunca para almacenar datos personales de PoC. Las cuentas corporativas locales o regionales no deben utilizarse sin la autorización por escrito

[31] *Véase, https://www.kobotoolbox.org/.*

[32] *Está previsto que la Biblioteca de Datos Internos en Bruto (RIDL) del ACNUR se confirme como un repositorio de datos interno seguro al que puedan acceder todos los miembros del personal del ACNUR y que pueda albergar todo tipo de datos operativos en todas las unidades de medida. Aunque el objetivo principal de la RIDL será el almacenamiento de datos no personales, cuando no sea posible transferir los datos personales a PRIMES, se espera que la RIDL proporcione esa capacidad de almacenamiento. La RIDL se someterá a nuevas evaluaciones en 2021 y se dispondrá de más detalles en la próxima versión de la Guía Interna.*

del controlador de datos de la operación en el país o, para el tratamiento de datos personales de PoC a nivel regional, sin la autorización del controlador de datos regional. Se anima a los controladores de datos a que pidan recomendaciones al DPO y CISO antes de autorizar el uso de dichas plataformas.

6.6.2 La operación de país y la entidad regional o de la sede deben llevar a cabo una DPIA antes de comprar, construir, utilizar o adaptar otras plataformas de almacenamiento para el almacenamiento de datos personales de las PoC. Los controladores de datos son responsables de organizar y llevar a cabo la DPIA (4.5.3 DPP) y de mantener informado al DPO (4.5.4 DPP).

6.6.3 El controlador de datos, asistido por el Punto Focal de Protección de Datos, también debería establecer procedimientos operativos estándar (SOP) para el uso de otras plataformas de almacenamiento. Por ejemplo, los SOP deben establecer las jerarquías de las carpetas en dichas plataformas de almacenamiento de acuerdo con la función y la estructura de la operación o entidad, y garantizar que los derechos de acceso a las carpetas funcionales se conceden a los miembros del personal en función de la "necesidad de saber".

6.6.4 En el caso de las iniciativas del Buró Regional que vayan a desplegarse en varios países de una región, deberá realizarse una evaluación de riesgos sobre la ciberseguridad de cada nueva plataforma de almacenamiento, que podría formar parte de la DPIA específica del país que se lleve a cabo a nivel de operaciones nacionales. Toda nueva plataforma de almacenamiento en el terreno, regional o en la sede debe ofrecer un cifrado completo de extremo a extremo y una MFA.

7. Almacenamiento fuera de línea y dispositivos móviles

7.1 Recomendaciones generales

7.1.1 El "almacenamiento fuera de línea" se refiere a cualquier medio de almacenamiento que debe ser insertado o cargado físicamente en un ordenador o dispositivo cuando un usuario quiere acceder a los datos o editarlos. Algunos ejemplos son los discos duros internos y externos extraíbles, los DVD (Digital Versatile Disk), los SSD (Solid-state drive) y las unidades USB (Universal serial bus).

7.1.2 Por "dispositivo móvil" se entiende un dispositivo informático portátil que está diseñado para ser fácilmente transportable, para funcionar sin una conexión física (por ejemplo, que transmite o recibe información de forma inalámbrica) y que almacena y procesa datos locales no extraíbles.[33] Los dispositivos móviles incluyen los ordenadores portátiles expedidos por ACNUR, los dispositivos Apple y Android y, para simplificar, los ordenadores domésticos.

[33] *Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en inglés) de Estados Unidos,* Laboratorio de Tecnología de la Información, Centro de Recursos de Seguridad Informática: Glosario, *disponible en inglés en: https://csrc.nist.gov/glossary/term/mobile_device.*

7.1.3 Esta Guía Interna **recomienda encarecidamente** que no almacenen datos personales de PoC en cualquier medio de almacenamiento externo no cifrado o dispositivo móvil. La pérdida del medio o del dispositivo podría dar lugar a una filtración de los datos personales que, si es explotada por partes hostiles (hackers, agencias de seguridad), podría suponer riesgos significativos o graves para la seguridad, la protección y/o los derechos fundamentales de las PoC individuales o de las comunidades afectadas. [34]

7.1.4 Cuando el personal de ACNUR necesite almacenar datos personales de las PoC en el disco duro de un ordenador de oficina, deberá hacerlo sólo si está protegido con BitLocker. BitLocker es una función de encriptado incluida en Microsoft Windows 10. [35]

7.1.5 Cuando los datos personales de las PoC se almacenan en medios de almacenamiento externos fuera de línea y/o en sistemas de TI no corporativos, ya sea en Excel, Word, PDF, imágenes escaneadas o cualquier otro formato de datos, el personal de ACNUR debe hacerlo sólo si los datos personales de las PoC se almacenan en dispositivos que están protegidos con una herramienta o servicio de encriptación BitLocker o equivalente, y que la contraseña cumple con la norma de ACNUR. Para verificar si un dispositivo está debidamente encriptado o protegido, el personal del ACNUR debe pedir consejo al punto focal de TI de su operación, al personal regional de TI o a CISO.

7.2 Asesoría específica sobre los dispositivos móviles

7.2.1 El uso de ordenadores y otros dispositivos TI por parte del personal de ACNUR está regulado por la Instrucción Administrativa sobre Informática para Usuarios Finales[36] y la Instrucción Administrativa sobre Gestión de Controles de Acceso a Sistemas, Aplicaciones y Servicios Tecnológicos. [37]

7.2.2 La aplicación de un código de acceso encripta automáticamente los datos almacenados en un iPad o iPhone. Otros teléfonos modernos (como los dispositivos Samsung) también tienen cifrado por defecto. Los dispositivos móviles (p. ej., teléfonos, tabletas) utilizados para almacenar y procesar datos personales de las PoC no deben tener un código de acceso trivial (p. ej., 000000). Los miembros del personal deben guardar de forma segura las contraseñas o códigos de acceso a un dispositivo y por separado del mismo.

7.2.3 Los dispositivos móviles no deben estar con **"bandas abiertas"**.[38] Un dispositivo con “bandas abiertas” permite la instalación de aplicaciones y la eliminación de las

---

[34] *Véase el apartado 7.2 de la DPG.*

[35] *ACNUR,* herramienta de cifrado de disco BitLocker*, octubre de 2019, disponible en inglés en: https://intranet.unhcr.org/en/support-services/ict-operations/dist-faq-search/bitlocker-disk-encryption--installing-and-using-the-tool.html.*

[36] *ACNUR,* Instrucción administrativa sobre informática para usuarios finales, ACNUR (UNHCR/AI/2019/13), *2019, disponible en inglés en: https://intranet.unhcr.org/content/dam/unhcr/intranet/policy-guidance/en/2019/UNHCR-AI-2019-13%20End%20User%20Computing.pdf.*

[37] *ACNUR,* Instrucción administrativa sobre la gestión de los controles de acceso a los sistemas, aplicaciones y servicios de TIC, ACNUR (ACNUR/AI/2018/4), *2018, disponible en inglés en: https://intranet.unhcr.org/content/dam/unhcr/intranet/policy-guidance/en/2018/Administrative%20Instruction%20o n%20Access%20Controls%20Management.pdf.*

[38] *Esto significa saltarse las restricciones que el fabricante puso en el sistema operativo y tomar el control total del dispositivo.*

protecciones de seguridad integradas en el sistema operativo, lo que supone un riesgo inaceptable.

7.2.4 Los miembros del personal que almacenen temporalmente datos personales de PoC en un dispositivo móvil personal, por ejemplo, datos recolectados en KoBo utilizando un teléfono o una tableta, deben transferir rápidamente dichos datos a una unidad oficial y destruir la copia en el dispositivo móvil inmediatamente después. Esto también incluye los correos electrónicos que contengan datos personales de PoC. Esta Guía Interna recomienda encarecidamente que se exija a los miembros del personal que declaren cualquier uso de dispositivos móviles personales para el almacenamiento de datos personales de PoC a su supervisor.

8. Comunicación y transferencia de datos segura (datos "en tránsito")

8.1 Encriptación

8.1.1 Toda comunicación de datos personales de PoC por medios electrónicos debe realizarse utilizando un protocolo de **encriptado** ("cifrado de extremo a extremo").[39] El cifrado de extremo a extremo restringe la capacidad de terceros para interceptar las comunicaciones entre un remitente y un destinatario, y por lo tanto reduce en gran medida el riesgo de filtración de los datos personales, es decir, el acceso no autorizado por parte de piratas informáticos, delincuentes comerciales o agentes estatales o cuasi estatales.

8.2 Comunicación interna - Generalidades

8.2.1 Para la comunicación de datos personales de PoC dentro de ACNUR (es decir, entre el personal de ACNUR, independientemente de su lugar de trabajo, se recomienda al personal de ACNUR que utilice plataformas oficiales para la transferencia interna, como el correo electrónico interno (Outlook), Microsoft Teams, e-SAFE y SharePoint. Todos estos productos están cifrados de extremo a extremo utilizando varias técnicas diferentes.[40]

8.2.2 Cuando se utiliza el sistema de correo electrónico de ACNUR, se recomienda evitar incluir datos personales de las PoC en el asunto y/o en el cuerpo de un correo electrónico. Aunque el correo electrónico interno dentro del dominio unhcr.org está cifrado por defecto, su flujo puede ser visto y el correo puede ser leído por un pequeño grupo de administradores. En general, es más seguro adjuntar los datos personales de las PoC en archivos protegidos por contraseña, por ejemplo, para evitar que un destinatario reenvíe

[39] *Véase, por ejemplo, Intersoft Consulting,* GDPR: Cuestiones Clave - Cifrado, *disponible en inglés en: https://gdpr-info.eu/issues/encryption/.*

[40] *Véase Microsoft,* Microsoft 365: Comprender el Cifrado, *2019, disponible en inglés en: https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption?view=o365-worldwide#:~:text=With%20Office%20365%2C%20your%20data%20is%20encrypted%20at,for%20data%20at%20rest%20and%20data%20in%20transit y* Microsoft 365: Cifrado para Teams, *disponible en inglés en: https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide#encryption-for-teams.*

accidentalmente el mensaje a terceros. Las contraseñas deben cumplir con las directrices sobre gestión de contraseñas de ACNUR. [41]

8.3 Comunicación externa - Generalidades

8.3.1 Las transferencias de datos personales de las PoC a socios externos (por ejemplo, terceros o socios del proyecto) no deben realizarse a través de correo electrónico no protegido. Siempre que sea apropiado, estas transferencias deben tener lugar a través de la Plataforma de Transferencia de Datos (DTP, por sus siglas en inglés) de PRIMES o concediendo un acceso limitado y controlado a PRIMES (por ejemplo, aplicando el Perfil de Socio a proGres v4).

8.3.2 Cuando el acceso a las herramientas PRIMES no es viable, las transferencias de datos personales de las PoC a socios externos con soporte para Protocolos de Transferencia de Archivos (FTP, por sus siglas en inglés) punto a punto pueden realizarse a través de un FTP seguro[42] o a través del sistema de Intercambio Seguro de Archivos (SFS, por sus siglas en inglés) del ACNUR.[43] Hay que tener en cuenta que el SFS sólo permite transferencias unidireccionales del ACNUR a un socio externo.

8.3.3 Cuando ni la DTP ni el Seguro FTP ni el SFS puedan soportar la transferencia de datos requerida, el personal del ACNUR podrá transferir archivos ZIP (con 7-Zip o WinZip) con protección por contraseña. El uso de contraseñas debe estar en consonancia con las directrices de ACNUR sobre la gestión de contraseñas. [44] La selección de los algoritmos también debe estar en consonancia con las orientaciones, ya que algunas de las opciones más "ligeras" pueden ser descifradas. El envío por correo o la transferencia de archivos ZIP de datos personales de las PoC no debe hacerse nunca sin protección por contraseña.

8.3.4 También pueden utilizarse memorias USB cifradas si el dispositivo está cifrado con Bitlocker de acuerdo con las directrices del ACNUR y se registra la contraseña. No se recomienda utilizar varias memorias USB de este modo.

8.3.4 Las contraseñas deben enviarse siempre por un canal distinto al utilizado para transferir los datos personales de las PoC. Por ejemplo, envíe la contraseña por SMS, Teams Chat o Signal si el archivo se envía por correo electrónico. De lo contrario, cualquiera que "hackee" el correo electrónico también puede obtener la contraseña.

8.3.5 Las operaciones de país y las entidades regionales y de la sede no deben utilizar nunca otras plataformas gratuitas de transferencia de datos en línea para la transferencia de datos personales de las PoC sin la autorización del Controlador de Datos. Estas

---

[41] *ACNUR*, Nota de orientación sobre la gestión de contraseñas, *abril de 2020, disponible en inglés en: https://intranet.unhcr.org/content/dam/unhcr/intranet/staff%20support/information-communication-technology/documents/english/Password%20Management%20Guidance.pdf.pdf.*

[42] *ACNUR*, File Sharing via FTP (Intercambio de archivos a través de FTP), *septiembre de 2017, disponible en inglés en: https://intranet.unhcr.org/en/support-services/ict-operations/ict-services/collaboration/file-sharing.html.*

[43] *ACNUR*, Safer File Sharing (Uso compartido más seguro de archivos), *noviembre de 2018, disponible en inglés en: https://intranet.unhcr.org/en/support-services/ict-operations/news--updates---events/safer-file-sharing.html.*

[44] *ACNUR*, Guidance Note on Password Management (Nota de orientación sobre la gestión de contraseñas), *abril de 2020, disponible en inglés en: https://intranet.unhcr.org/content/dam/unhcr/intranet/staff%20support/information-communication-technology/documents/english/Password%20Management%20Guidance.pdf.pdf.*

plataformas incluyen WeTransfer, Dropbox, Boot Camp, Apple iCloud y Google Drive y Forms.

8.3.6 De acuerdo con el párr. 4.5.1 de la DPP, una operación de país y una entidad regional o de la sede deben realizar una DPIA antes de utilizar otras plataformas de transferencia de datos en línea gratuitas para la transferencia de datos personales de PoC. Los Controladores de Datos son los encargados de organizar y llevar a cabo la DPIA (4.5.3 de la DPP) y de mantener informado al DPO (4.5.4 de la DPP).

8.4 Comunicación externa - Mensajería móvil

8.4.1 Cuando se utilice una aplicación de mensajería móvil para la comunicación y la transferencia de datos personales de las PoC (incluso directamente hacia y desde las propias personas de interés), se anima a las operaciones de países y a las entidades regionales y de la sede a utilizar Signal, la aplicación respaldada por las Naciones Unidas.[45]

8.4.2 Las operaciones de países y las entidades regionales y de la sede no deben utilizar otras aplicaciones de mensajería móvil que no estén avaladas por ACNUR (por ejemplo, WhatsApp) para las comunicaciones de datos personales de las PoC sin la autorización del Controlador de Datos. En estos casos, se debe realizar una DPIA[46]. Los Controladores de Datos son responsables de organizar y llevar a cabo las DPIA (4.5.3 DPP) y de mantener informado al DPO (4.5.4 DPP).

8.4.3 Los chats de grupo son intrínsecamente menos seguros que los chats 1-1, ya que existe el riesgo, si se descubren y explotan las vulnerabilidades, de que personas extrañas encuentren secretamente su camino en el chat. Compruebe siempre el número de asistentes a una llamada de chat.

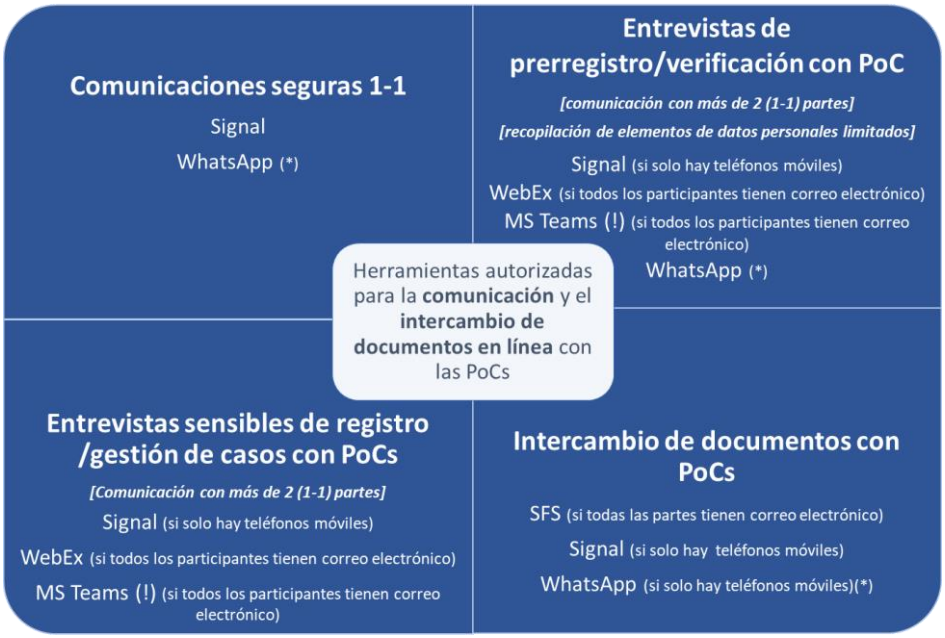
El siguiente cuadro ofrece orientación sobre las aplicaciones de comunicación en línea que podrían utilizar las operaciones en los países y las entidades regionales y de la sede.

Herramientas autorizadas para la comunicación y el intercambio de documentos en línea con las personas de interés

[45] *ACNUR*, Signal: Standard for Secure Mobile Communication (Signal: estándar para comunicación móvil segura), *Feb 2020, disponible en inglés en: https://intranet.unhcr.org/en/support-services/ict-operations/ict-services/collaboration/signal--standard-for-secure-mobile-communication.html.*

[46] *ACNUR, Using Social Media for Community-Based Protection: A Guide (Uso de las redes sociales para la protección comunitaria: una guía), enero de 2021, disponible en inglés en: https://www.unhcr.org/innovation/wp-content/uploads/2021/01/Using-Social-Media-in-CBP.pdf.*

Herramientas autorizadas para la comunicación y el intercambio de documentos en línea con las personas de interés



Notas explicativas:

(*) – WhatsApp es una alternativa permitida junto a *Signal* en el caso de que sea necesario comunicarse con un usuario existente de WhatsApp, y si el riesgo es aceptado por el Controlador de Datos.

SFS – Plataforma de Intercambio Seguro de Archivos para el intercambio unidireccional de archivos de ACNUR a un tercero. La plataforma requiere que se comparta un hipervínculo con la PoC mediante correo electrónico.

MS Teams (!) – Herramienta corporativa que permite la comunicación con parte(s) externa(s). Sin embargo, las direcciones de correo electrónico de los participantes **no se pueden** ocultar.

Signal – Estándares recomendados para la comunicación segura. Desde diciembre de 2020, Signal admite tanto el audio como el video en llamadas grupales (limitas a 5 participantes).

9. Contacto

Si desea obtener más asesoría o retroalimentación sobre esta guía interna, póngase en contacto con el Equipo de Protección de Datos del Servicio Global de Datos en HQDPOGDS@unhcr.org y con el Oficial Principal de Seguridad de la Información en DIST en CISO@unhcr.org.