HOJA DE RECOMENDACIONES SOBRE LA SEGURIDAD DE LOS DATOS EN LA GESTIÓN DE DATOS OPERATIVOS

OCHA CENTRE FOR HUMANITARIAN DATA

CartONG ha facilitado la traducción de esta hoja de consejos, gracias al apoyo de CLEAR Global y el Ministerio para Europa y de Asuntos Exteriores de Francia.

INTRODUCCIÓN

La seguridad de los datos es un componente clave en la responsabilidad de los datos: gestión segura, ética y eficaz de los datos para la respuesta operativa. Implica un conjunto de medidas físicas, tecnológicas y de procedimientos que salvaguardan la confidencialidad, integridad y disponibilidad de los datos y evitan su pérdida, destrucción, alteración, adquisición o divulgación accidental o intencionada, ilícita o no autorizada.

Esta hoja de recomendaciones ofrece una serie de acciones sugeridas para la seguridad de los datos en la gestión de datos operativos. Las acciones deben aplicarse de acuerdo con los mandatos institucionales, las políticas y los marcos jurídicos y reglamentarios pertinentes.

PRACTIQUE UNA BUENA GESTIÓN DE CONTRASEÑAS

- Proteja sus dispositivos y cuentas con contraseñas seguras que incluyan números, letras mayúsculas y minúsculas, y símbolos, con al menos 16 caracteres o más por contraseña.
- Habilite la autenticación multi-factor para todas las cuentas.
- No reutilice la misma contraseña para varias cuentas.
- No guarde sus contraseñas físicamente (por ejemplo, en notas) ni digitalmente (en un archivo de su dispositivo) y no las comparta con otras personas.
- No active la función "recordar contraseña" en aplicaciones y navegadores.
- Cambie inmediatamente las contraseñas de sus cuentas en línea si pierde o le roban su dispositivo.

UTILICE SOFTWARE ANTIVIRUS/ANTI-MALWARE

- Asegúrese de que dispone del software antivirus/anti-malware adecuado en sus dispositivos.
- Si tiene preguntas sobre las herramientas adecuadas o cómo configurarlas, consulte con el/la especialista en TI de su oficina.

MANTENGA ACTUALIZADOS EL SOFTWARE Y LOS SISTEMAS OPERATIVOS

- Compruebe regularmente que su dispositivo, software, aplicaciones y complementos del navegador estén actualizados y active las actualizaciones automáticas de su sistema operativo.
- Utilice navegadores web como Chrome o Firefox que reciben actualizaciones de seguridad automáticas.
- Apague los dispositivos al final del día para permitir la actualización y protegerse de ataques.

EVITE LAS ESTAFAS DE SUPLANTACIÓN DE IDENTIDAD (PHISHING) Y TENGA CUIDADO AL HACER CLIC

- Cuando reciba correos electrónicos o mensajes sospechosos, compruebe siempre la dirección o la información de contacto del remitente y sólo haga clic en los enlaces o archivos adjuntos si confía en quien los envía.
- No responda a correos electrónicos sospechosos ni los reenvíe a sus colegas.
- Informe de cualquier actividad sospechosa a su equipo de soporte informático.

UTILICE LOS DISPOSITIVOS MÓVILES DE FORMA RESPONSABLE

- En la medida de lo posible, utilice dispositivos exclusivos para fines laborales. Mantenga sus dispositivos de trabajo, en un lugar seguro en todo momento, y evite llevarlos consigo innecesariamente.
- Utilice herramientas de mensajería aprobadas por su organización que proporcionen cifrado de extremo a extremo.
- Desactive la conectividad Bluetooth siempre que sea posible y reduzca al máximo el uso de la conectividad Bluetooth.
- Utilice una Red Privada Virtual (VPN), aprobada por su organización, cuando trabaje en línea. Cierre siempre la sesión de su(s) cuenta(s), si está utilizando un ordenador o dispositivo público.
- Desactive las funciones de desbloqueo biométrico, especialmente cuando se está viajando.

PROTEJA LOS DATOS CONFIDENCIALES Y PRACTIQUE LA MINIMIZACIÓN DE DATOS

- Mantenga un registro de activos de datos que indique el nivel de sensibilidad de cada tipo de dato gestionado por su oficina. Revise periódicamente los niveles de confidencialidad, a medida que evolucione el contexto.
- Recopile la cantidad mínima de datos necesaria para alcanzar el objetivo y los fines de una determinada actividad de gestión de datos.
- Conserve los datos sensibles sólo durante el tiempo necesario para cumplir la finalidad para la que se gestionaron y según lo exigido por las directrices, leyes y reglamentos aplicables.
- Transfiera y almacene los datos utilizando herramientas y canales aprobados por su organización (un servidor local de la organización, ordenador o portátil de la organización; o en servidores y sistemas operados remotamente a través de aplicaciones como OneDrive, SharePoint y Teams).
- Proteja con contraseña los archivos (Word, Excel, PDF) que contengan datos confidenciales y comparta las contraseñas de los documentos a través de canales diferentes (por ejemplo, envíe por mensaje de texto la contraseña para un documento que fue enviado por correo electrónico).
- Limite y controle cuidadosamente el número de personas con acceso a datos confidenciales.
- Defina un calendario de conservación y destrucción para todos los datos gestionados y utilice las herramientas adecuadas para la destrucción de datos.
- Encripte sus mensajes de correo electrónico.

PRINCIPALES RECURSOS

- **Guía operativa del IASC sobre la responsabilidad de los datos en la acción humanitaria**
- **Nota orientativa sobre la gestión de incidentes con datos**
- **Hoja de sugerencias sobre el uso responsable de las herramientas de conferencia en línea**

Si desea más información sobre la gestión de datos sensibles en operaciones humanitarias, visite la página de Responsabilidad de los datos en el sitio web del Centro o póngase en contacto con nuestro equipo en centrehumdata@un.org.