



Protección de datos

Un breve resumen



DEFINICIÓN

Conjunto de principios y prácticas para asegurar que los datos personales sean recopilados, usados y protegidos de manera que se tenga en consideración la privacidad del individuo y cualquier riesgo que pueda ocurrir por no proteger adecuadamente sus datos.

CONCEPTOS



Procesamiento: operaciones con información personal incluyendo recopilación, almacenamiento, acceso, análisis, eliminación, etc.



Datos personales: información que se refiera a una persona física viva que sea identificable o pueda ser identificada: nombre, dirección, género, edad, número de identificación, foto, huella dactilar, etc. También información más delicada: condiciones de salud o religiosas, afiliaciones políticas o orientación sexual. Es importante remarcar que esta lista no es definitiva: lo que es personal y lo que es delicado puede cambiar dependiendo del contexto político, social o económico.



Compartir: facilitar acceso a información al enviarla por email, al proporcionar un enlace a información digital, al hacer una copia y dársela a alguien, o al facilitar acceso directo o indirecto a una base de dato.

MEJORES PRÁCTICAS GERALES



CORRECTO

- Determinar qué información es completamente necesaria recopilar antes de implementar un proyecto.
- Tener en cuenta las tradiciones locales y el contexto político al determinar qué información personal recopilar, y cómo explicar el motivo o motivos de dicha recopilación.
- Considerar que los datos demográficos y de localización pueden ser delicados, incluso aunque no sean personales, y que pueden poner en peligro a personas o a grupos.
- Decidir qué información se le proporcionará a las personas afectadas. Por ejemplo: el objetivo del proyecto, por qué se tienen que recopilar datos, cómo se usarán y con quién se compartirán, o adónde ir en caso de tener preguntas sobre su información personal.
- Al proporcionar información o al obtener consentimiento, realizar un registro de las interacciones, incluyendo: qué información se ha proporcionado, quién la ha facilitado, la fecha, el lugar, el destinatario, o si ha habido alguna queja.
- Determinar quién será el responsable de responder a las preguntas sobre el uso, almacenamiento, corrección, etc. de la información.
- Encriptar y/o proteger con contraseñas aparatos electrónicos y cualquier archivo digital (Word, Excel, etc.) que contenga datos personales o delicados.
- Planear qué pasará con la información personal una vez que ya no vaya a usarse. Por ejemplo, ¿se archivará, o se puede destruir o eliminar de forma segura?
- Solo proporcionar acceso a archivos físicos o digitales que contengan información personal a los empleados (o voluntarios, asesores u otros agentes autorizados) que necesiten acceso para realizar su trabajo.
- Mantener contraseñas, cerraduras, candados físicos, antivirus, firewalls y cualquier otra forma razonable de seguridad para ordenadores, dispositivos móviles, archivadores, u otros lugares dónde se almacenarán datos personales.
- Planear un acuerdo por escrito antes de compartir fuera de su organización cualquier dato personal o delicado.



INCORRECTO

- Usar carpetas públicas de Dropbox, Drive/Docs de Google que sean de acceso público o cualquier otra plataforma de Internet para compartir o colaborar en documentos que contengan información personal o delicada, especialmente cuando esos archivos no estén protegidos por contraseñas.
- Compartir o facilitar el acceso a archivos que contengan información personal a gobiernos o a cualquier otro socio sin considerar primero las consecuencias de no formalizar los términos dicha acción.
- Publicar en redes sociales detalles personales (fotos incluidas) sobre las personas afectadas, ya sea de manera personal o profesional, sin el previo acuerdo de los equipos legales y de comunicación de su organización.
- Dejar archivos con información personal o delicada al alcance. Guárdalos bajo llave en armarios, escritorios, u oficinas cuando no se usen.
- Usar dispositivos de almacenamiento USB para la información personal o delicada, a menos que su contenido esté encriptado o protegido por contraseña.
- Asumir que el simple hecho de preguntar por el consentimiento de un individuo, o que estén de acuerdo con el hecho de que se use su información personal es moral y legalmente suficiente para actuar. No se puede dar consentimiento libremente cuando se está condicionado por la necesidad de ayuda.



Por favor, tenga en cuenta que esta ficha no provee una información completa. Hay muchas áreas de la protección de datos que no se han cubierto aquí. Busque siempre asesoramiento legal cuando tenga preguntas sobre la interpretación y/o implementación de las prácticas de protección de datos.



Preparado por la oficina de PD de FICR.

Información
del contacto :

Gestión de la información
FICR HQ, Ginebra
im@ifrc.org