# Gestión responsable de datos: Manual para los formadores




irct
International Rehabilitation Council for Torture Victims

Ministry of Foreign Affairs of the Netherlands

# Contenido

# Acerca del manual

*Este documento ha sido elaborado como parte del proyecto Global Anti-Torture Evidence (GATE) [Evidencia Mundial Contra la Tortura] del IRCT, financiado generosamente por el Ministerio de Relaciones Exteriores de los Países Bajos. Este manual está destinado a utilizarse como referencia para trabajos profesionales en centros de rehabilitación de torturados con el objeto de formar a otras personas en el tema de la recogida responsable de datos. Presenta una introducción y ejercicios prácticos en el ámbito de gestión ética y responsable de los datos en el contexto de los derechos humanos y de la lucha contra la tortura. Puede utilizarse como una herramienta independiente o conjuntamente con otros recursos que se empleen en la gestión responsable de datos.*

Este documento fue escrito por Carrie Gaston.

## 1. Introducción

La información es una parte esencial de cualquier organización y uno de sus bienes más valiosos. La gobernanza de la información y las técnicas de la manipulación responsable de datos constituyen un marco de referencia para el manejo de dicha información. Se trata, en particular, del manejo de la información sobre ***personas identificables*** y de la información ***confidencial*** de un modo seguro, confidencial y *consciente*.

Toda persona que trabaje para una organización o en nombre de ella debe ser consciente de lo siguiente:

- La importancia de la información conservada que pueda ser confidencial o sensible y que se relacione con los usuarios de sus servicios, su personal, sus voluntarios, donantes y patrocinadores o cualquier otra persona asociada con su organización.
- La legislación pertinente en los países en los que opera, así como las orientaciones pertinentes y las prácticas óptimas para velar por esta importante información.
- ¿Por qué debe USTED asumir la responsabilidad de cómo obtener, registrar, utilizar, conservar y compartir información?
- El impacto que la gestión responsable de los datos tiene en la continuidad de las actividades y en la capacidad para seguir prestando un servicio seguro y fiable a las personas a las que presta asistencia.

***¡La gestión responsable de los datos es responsabilidad de todos!***

# 2. Datos: Identificación de los diferentes tipos de datos

*En esta sección, enseñará a los participantes los distintos tipos y categorías de datos, cómo identificar estos tipos y categorías, así como los riesgos y protecciones que se vinculan con cada uno de ellos.*

*Objetivos de aprendizaje: al final de esta sección, los participantes:*

- *Podrán identificar las distintas categorías de datos.*
- *Comprenderán los posibles riesgos vinculados con las distintas categorías de datos.*
- *Pensarán en cómo aplicar protecciones a los distintos tipos de datos en sus propios contextos.*
- *Tendrán conocimientos sobre la anonimización de datos personales.*

## Tipos de datos

En cada contexto organizativo, pero particularmente en cualquier tipo de organización que se ocupe de la atención sanitaria y social, entramos en contacto con diversos tipos de información personal sobre las personas.

Es importante poder identificar estos distintos tipos de información para poder protegerlos adecuadamente a la hora de utilizarlos y compartirlos.

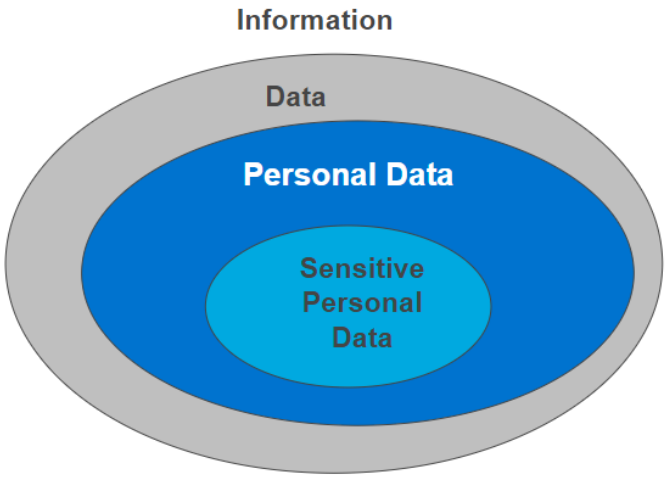
Se entiende por ***información*** cualquier conjunto de hechos acerca de algo, que se proporciona o de los que alguien se entera.

Los ***datos*** son un conjunto de valores de variables cualitativas o cuantitativas.

Los ***datos personales (DP)*** son datos relativos a una persona viva e identificable:

- a partir de esos datos;
- a partir de esos datos y otros elementos de información que estén en posesión de la persona física o jurídica («responsable del tratamiento» según la terminología aplicable a la protección de datos).

***Datos personales sensibles (DPS)***: Es una categoría especial de datos personales que se relaciona con el origen racial o étnico, las opiniones políticas, las creencias religiosas u otras similares, la afiliación sindical, el estado de salud física o mental, la vida sexual, la comisión o presunta comisión de algún delito.



La ***información confidencial*** es una información sobre la que existen sensibilidades en torno a su manejo y a su divulgación. Puede tener un carácter personal u organizativo. Por lo general, los *datos personales sensibles* deben tratarse siempre como confidenciales; sin embargo, no toda información confidencial tiene un carácter sensible o personal. Por ejemplo, la información empresarial crucial puede ubicarse en esta categoría.

Además de pensar acerca de cómo usted y su organización pueden *proteger* los datos de una violación externa a su organización, también merece la pena pensar acerca de cómo aplicar buenas prácticas en el tratamiento confidencial de los datos tanto externamente como *dentro de* su organización. Esto puede significar que, junto con esta formación, usted piense acerca de la aplicación de políticas y procedimientos organizativos que aporten a su personal una orientación sobre las buenas prácticas de manejo de cualquier cosa que pueda considerarse información confidencial. Esto podría traducirse en el diseño de una Política de confidencialidad o de un Código de conducta para el personal.

*Pregunte a los participantes si pueden pensar en algún tipo de información en sus propios contextos que pueda ubicarse en esta categoría. Pida a los participantes que hagan una lista en un papel con esta información y que piensen acerca de las protecciones que puedan tener establecidas, tanto para identificar como para proteger la categoría de información en cuestión. Una vez que hayan terminado, conversen sobre los ejemplos que escribieron los participantes.*


*El siguiente es un ejercicio de clasificación de datos. Pida a los participantes que clasifiquen una lista de posibles conjuntos de datos en 3 categorías, identificándolas como personal, sensible o ninguna de las dos. La lista dada es en sí intencionalmente vaga, de tal manera que los participantes se animen a formular las preguntas adecuadas sobre los datos dados y sientan que tienen toda la información necesaria para etiquetar el elemento como personal o sensible. El ejercicio debe suscitar un debate sobre conjuntos de datos personales*

*y sensibles, de tal manera que se afiancen los conocimientos que tengan los participantes sobre las distintas definiciones.*

*Siempre que sea posible, repita el ejercicio con versiones físicas reales de distintos conjuntos de datos que se utilicen en el contexto local. Al final del ejercicio los participantes deberán ser capaces de:*

*-diferenciar entre datos personales, datos personales sensibles y datos que no sean ni personales ni sensibles.*

## Ejercicio 1: Comprensión de los diferentes tipos de datos

*Estos son algunos ejemplos de distintos conjuntos de datos y elementos de información. Pida a los participantes que los coloquen en la categoría adecuada: sensible, personal, ninguna de las dos. Pídales que piensen si los elementos que no son ni personales ni sensibles deben seguir tratándose como «confidenciales».*

*Asimismo, pídales a los participantes que piensen si necesitan alguna información adicional para determinar la categoría adecuada y tome nota de sus preguntas.*

| **Datos personales sensibles** | **Datos personales** | **Datos (ni DP ni DPS)** |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

detalles de las tarjetas de crédito de una lista de donantes recientes;

una lista que contenga la información de salud mental de los pacientes de una clínica;

nombres y direcciones de clientes;

documentos que contengan los primeros 10 idiomas de su cartera de clientes y el número de hablantes de cada idioma;

lista de clientes y su afiliación política en la que no se utilicen los nombres, pero sí los números de identificación;

datos demográficos agregados de todos los clientes que hayan acudido al centro durante el último año;

| | | |
|---|---|---|
| una lista de los 350 clientes que acudieron durante el último año, así como su origen étnico y su orientación sexual; | resultados de una encuesta anónima; | una lista de direcciones de correo electrónico de los clientes que asistieron a un grupo del viernes; |
| información sobre los resultados relativos a una población de clientes, por ejemplo sus puntuaciones y los cambios en sus puntuaciones en una medición de salud mental estándar; | fotocopias de los pasaportes de diversas personas; | información sobre las comisarías y centros de detención nombrados por los clientes como lugares en los que han estado detenidos; |
| estadísticas sobre los cinco principales métodos de tortura y tratos inhumanos acerca de los cuales sus clientes le han hablado desde la inauguración de su centro hace 5 años; | una lista de todas las religiones a las que están afiliados sus clientes | un informe interno con información empresarial sensible. |

**¿Por qué es importante proteger la información personal?** Es importante cumplir con la legislación y las mejores prácticas que se aplican para proteger la *información personal* porque la información personal y la información sensible es valiosa. La manipulación y protección inadecuadas de los datos puede causar daños personales, sociales y a la reputación. En nuestro propio contexto de rehabilitación de la tortura, los riesgos pueden ser incluso mayores e implicar la seguridad personal de las personas que acuden a nuestros servicios.

**Formas comunes de pérdida de información:**

- Pérdida de información (inclusive registros en papel) por teléfono, por fax, pérdida de equipos informáticos o dispositivos móviles.
- Robo de información, inclusive por medio de ataques de phishing (suplantación de identidad) (véase el Glosario).
- Almacenamiento y eliminación inseguras de información que dé lugar a pérdida o robo.

**El error humano es más perjudicial que los ataques cibernéticos**

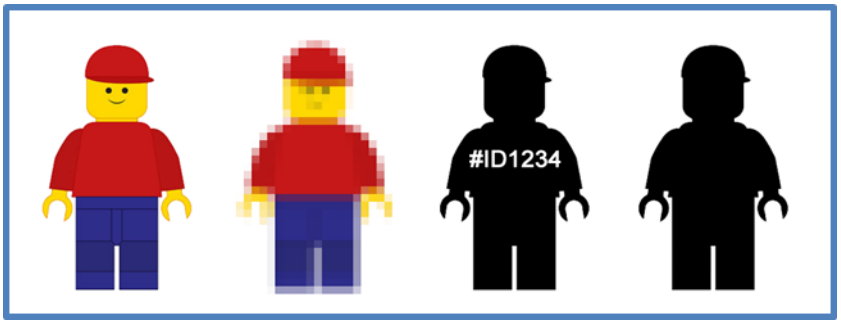
De octubre a diciembre de 2017, los errores humanos representaron casi dos tercios de los incidentes informados a la Oficina del Comisionado de Información (**ICO**) del Reino Unido, el organismo independiente creado para defender los derechos relativos a la información. Los errores humanos causaron más pérdidas o daños que las páginas

web inseguras y el *hacking*, que, sumados, ascienden solo a un 9%. A pesar de ello, la atención y los recursos del mercado siguen centrándose en las amenazas externas, en particular los ataques cibernéticos y los *hackers*.

- La clasificación que hace el ICO de los tipos de violaciones causadas por errores humanos revela las principales causas, tales como:
  - datos enviados por correo electrónico a un destinatario equivocado (15,8%);
  - pérdida y robo de documentos (13,1%);
  - datos enviados por correo o por fax a un destinatario equivocado (13,0%).

- Entre las demás causas figuran la eliminación insegura de equipos y documentos, la pérdida o el robo de dispositivos sin cifrar y la no supresión de datos.

## Omitir el término «personales» de «datos personales»: Anonimización y seudonimización




La **seudonimización** es el procedimiento mediante el cual la mayoría de los campos de identificación de un registro de datos se sustituyen por uno o más identificadores artificiales o seudónimos. Puede haber un único seudónimo para un conjunto de campos sustituidos o un seudónimo por cada campo sustituido. Esto ayuda a ocultar la identidad de la persona en la vida real, ***pero*** no constituye una verdadera anonimización ya que la identidad puede descubrirse con facilidad si se tiene acceso a la clave que se haya utilizado para la codificación.

| | | |
|---|---|---|
| Nombre: Alisha Santos<br>Fecha de nacimiento: 21 de abril de 1980<br>Educación: Licenciatura Psicología, Universidad de Guelph | seudonimización | ID#357986<br>Fecha de nacimiento: 21/04/1980<br>Educación (nivel máximo): 4<br>Lugar de nacimiento: Cataratas del Niágara, Ontario, Canadá |

| | |
|---|---|
| Lugar de nacimiento: Cataratas del Niágara, Ontario, Canadá<br>Empleo actual: Profesor de Matemáticas en la Universidad de Cambridge<br>Estado civil: casada con Dean O'Donnell<br>Número de hijo(a)s: 3 | Empleo actual: Profesora<br>Estado civil: Casada<br>Hijo(a)s: y |

La **anonimización** es el proceso de convertir los datos de forma tal que no se identifique a las personas físicas y en el que sea improbable que se lleve a cabo la identificación. Esto permite un uso más amplio de la información.

«Utilizamos el término "información anónima" para referirnos a datos que no identifiquen a ninguna persona física, y que sea poco probable que permita que se identifique a alguna persona física mediante su combinación con otros datos» (código de práctica de la anonimización de ICO, pg. 6)

| | | |
|---|---|---|
| Nombre: Alisha Santos<br>Fecha de nacimiento: lunes, 21 de abril de 1980<br>Educación: Licenciatura Psicología, Universidad de Guelph<br>Lugar de nacimiento: Cataratas del Niágara, Ontario, Canadá<br>Empleo actual: Profesor de Matemáticas en la Universidad de Cambridge<br>Estado civil: casada con Dean O'Donnell<br>Número de hijo(a)s: 3 | anonimización | Núm. de Id. 357986<br>Grupo de edad: 30-40<br>Educación (nivel máximo): Título<br>Lugar de nacimiento: Ontario del Sur, Canadá<br>Empleo actual: maestra<br>Estado civil: casada<br>Hijo(a)s: sí |

## Unas breves palabras sobre la agregación...

La **agregación de datos** es el proceso mediante el cual la información se recopila y expresa de manera resumida, para fines tales como el análisis estadístico. Cuando los

datos no son de ***personas identificables*** no están sujetos a las mismas protecciones legislativas, aunque podrían seguir siendo sensibles desde un punto de vista comercial y, por ende, seguir requiriendo protección (véase *información confidencial* arriba).

*El siguiente ejercicio ayudará a los participantes a reflexionar acerca de cómo sus propios datos en sus propios contextos se refieren a las categorías de datos que se mencionan anteriormente. La parte b) del ejercicio ayudará a los participantes a reflexionar acerca de cómo pueden proteger determinadas categorías de datos, mediante el uso de, por ejemplo, técnicas de anonimización. Al final del ejercicio los participantes deberán ser capaces de:*

*-enumerar los conjuntos de datos en su propio contexto;*

*-identificar esos conjuntos de datos como datos personales o no;*

*-debatir en torno a cuáles datos puede conservar su organización que no sean datos personales pero que aún necesiten tratarse como confidenciales.*

*-empezar a pensar acerca de la aplicación de protecciones a los distintos tipos de datos.*

*-pensar en cómo aplicar la anonimización a los datos personales antes de compartirlos.*

*-posiblemente comenzar a pensar en acuerdos de intercambio de datos.*

## Ejercicio 2: Comprender los distintos tipos de datos en su propio contexto.

*a) Enumeren conjuntos de datos comunes que ustedes traten (recojan, gestionen, informen, almacenen, etc.) e intenten clasificarlos en las diferentes categorías que se analizaron anteriormente (datos personales (DP), datos personales sensibles (DPS), ninguno de los dos). ¿Alguno de esos conjuntos de datos son potencialmente "confidenciales", pero que no encajan en la categoría "personales"? ¿Los riesgos asociados con estos datos son diferentes? ¿Aplicarían las mismas medidas de protección xxx a este tipo de datos?*

*b) Piensen en un conjunto de datos con el que trabajen (por ejemplo, una lista de clientes) que necesite compartirse. ¿Pueden pensar en cómo pueden proteger esta información tanto como sea posible antes de compartirla?*

# 3. La protección de datos en la legislación (UE)

*En esta sección, usted presentará el marco legislativo de la protección de datos. Esta nueva legislación actualizada solo se aplica en la Unión Europea, pero es útil conocerla ya que representa, de diversas maneras, la «regla de oro» en materia de protección de datos. También es útil como una herramienta para aprender buenas prácticas, aun cuando la legislación no se aplique directamente en su zona particular del mundo.*

*Objetivos de aprendizaje: Al final de esta sección, los participantes:*

- *Tendrán un conocimiento de las leyes actuales que rigen la protección de datos en la Unión Europea;*
- *Tendrán un conocimiento de los derechos individuales de los interesados en materia de datos y de las responsabilidades de los responsables y de los encargados del tratamiento de dichos datos;*
- *Pensarán en cómo aplicar estos derechos y responsabilidades a sus propios datos en sus propios contextos;*
- *Comprenderán cómo realizar un ejercicio de asignación de datos para identificar qué datos se deben conservar y dónde;*
- *Entenderán qué es una «solicitud de acceso del interesado» y cómo cumplir con ella, incluida la supresión de datos;*

## El marco legislativo europeo: Una introducción al Reglamento General de Protección de Datos (RGPD)

El **Reglamento General de Protección de Datos** (RGPD) de la UE es una nueva legislación que se convierte en la única ley de privacidad de datos de la Unión Europea. Consolida y fortalece la legislación de protección de datos existente en los siguientes ámbitos clave:

Definiciones:

- Un «interesado» es toda persona cuyos datos personales sean tratados por su organización.
- Un «responsable del tratamiento» es la persona física o jurídica que determina los fines, las condiciones y los medios del tratamiento de los datos personales.
- Un «encargado del tratamiento» es la persona física o jurídica que trata los datos por cuenta del responsable del tratamiento.

➔ ***Derechos individuales***: En virtud del RGPD, los derechos del interesado se fortalecen o mejoran en una serie de ámbitos. Entre estos ámbitos figuran:

- **Derecho a ser informado**: Los interesados tienen derecho a saber qué se está haciendo con sus datos y quién lo hace.

- **Derecho de acceso**: Los interesados tienen derecho de acceso a los datos personales que usted conserve acerca de ellos, lo cual incluye suministrarles gratuitamente una copia de sus datos en un plazo razonable (*véase también* infra *sobre Solicitudes de acceso del interesado*).
- **Derecho de rectificación**: Los interesados pueden exigir cambios en los datos que usted conserve sobre ellos y que ellos consideren falsos, desactualizados o incompletos.
- **Derecho de supresión**: Los interesados tienen ahora el derecho a exigir que se suprima la información que les concierna; esto también se conoce como el «derecho al olvido».
- **Derecho a la limitación del tratamiento**: Los interesados pueden solicitar la suspensión o supresión del tratamiento de sus datos personales. En estas circunstancias, puede ser necesario que los encargados del tratamiento sigan almacenando datos relativos al interesado con el fin de respaldar lo anterior. (Un ejemplo de esto puede ser cuando un donante o simpatizante haya solicitado a una organización que deje de ponerse en contacto con él o ella para pedir apoyo monetario. Los datos que se conserven serían entonces aquellos que tuvieran el valor mínimo para respaldar la petición de dejar de ponerse en contacto con el interesado).
- **Derecho a la portabilidad de los datos**. Los interesados podrán obtener, trasladar o reutilizar sus datos en distintos servicios o para sus propios fines.
- **Derecho de oposición**: Los interesados tienen derecho a oponerse al tratamiento de sus datos, incluida la mercadotecnia o la elaboración de perfiles.
- **Derechos relacionados con las decisiones individuales automatizadas, incluida la elaboración de perfiles**: Existen requisitos específicos con el fin de cumplir con la legislación relativa a la toma de decisiones automatizadas.

➔ El RGPD también refuerza o mejora la ***rendición de cuentas de los responsables del tratamiento***, toda vez que se espera que establezcan medidas de gobernanza integral y promuevan la rendición de cuentas y la transparencia.

➔ Esto también incluye obligaciones de mayor alcance en el ***cumplimiento de los encargados del tratamiento***, incluidos los contratistas.

➔ También incluye ***obligaciones relativas a informar de las violaciones en materia de datos*** y a contar con una persona responsable de la protección de datos en las grandes organizaciones, los organismos públicos y en las entidades que lleven a cabo el tratamiento a gran escala de datos personales.

➔ Protección de datos desde el diseño y por defecto: Consiste en pensar en aplicar medidas para proteger los datos desde el diseño de cualquier nuevo sistema antes de que se lleve a cabo la recolección de datos.

➔ Evaluaciones de impacto en la privacidad: Prestar la debida atención a los posibles impactos en la privacidad de las personas físicas en todas las actividades de tratamiento.

## Unas breves palabras sobre las solicitudes de acceso del interesado…

En virtud de la legislación actual y que de la que se propone en materia de protección de datos, cualquier *interesado* tiene derecho a solicitar cualquier información personal que le concierna que esté en poder de cualquier organización. Esto implica que toda persona puede solicitar una copia de la información, o solicitar verla, que un responsable o encargado de tratamiento de datos conserve sobre ella; y el cumplimiento de esta solicitud no puede denegarse. Al cumplir con tal petición, es importante respetar los principios (derechos individuales) de los interesados, quienes podrían suprimir alguna información cuando esta haya sido obtenida de terceros y que forme parte del registro que usted conserva.

*Pídales a los participantes que piensen en cómo cumplirían con una solicitud de acceso de un interesado que utilice sus servicios. ¿Qué deberían considerar al cumplir con dicha solicitud? Pídales que piensen en ejemplos de registros que puedan contener información que deba suprimirse antes de cumplir con una solicitud. Debatir sobre estos ejemplos en grupo.*

## Asignación de datos

Para proteger adecuadamente los datos y cumplir con los puntos anteriores, lo primero que necesita saber es qué datos conserva y dónde los conserva. Es una buena idea realizar un ejercicio de asignación de datos, para que usted y los miembros de su organización sepan con claridad qué datos conservan, dónde se almacenan, durante cuánto tiempo se conservan y cuándo y cómo se destruyen.

Lo que debe tenerse en cuenta….

**¿QUÉ datos personales tiene?** Para responder a esta pregunta, deberá realizar un examen y una auditoría exhaustivos de TODOS los datos personales que usted recoja, por ejemplo:

- ¿Tiene información escrita en trozos de papel en un cajón de su escritorio?
- ¿Tiene información personal escrita en un diario de papel?
- ¿Puede cumplir con una solicitud de acceso de un interesado?

**¿DÓNDE se almacena?**

- ¿En una base de datos?
- ¿En unidades de red o compartidas? ¿Quién tiene acceso?
- ¿En diarios de papel? ¿En trozos de papel en su escritorio?
- ¿En casa? ¿En correos electrónicos?

**¿ADÓNDE se envía?**

- ¿Puede confirmar que solo envía información sobre clientes hacia ubicaciones de su propio país?
- ¿Cuenta con un permiso explícito, escrito o documentado para enviar los datos? ¿Puede presentar prueba de ello?

**¿CÓMO se tratan los datos?**

- ¿En ordenadores?
- ¿En trozos de papel?
- ¿Cómo protege los datos en tránsito?

**¿QUÉ comunica a las personas o interesados acerca del tratamiento de los datos que usted conserva**?

- ¿Tiene información plenamente disponible para los interesados?
- ¿Identifica a los encargados del tratamiento de terceros?
- ¿Los datos cruzan fronteras nacionales o internacionales?

Garantía de protección de la información clínica: ¿Es la información correcta? ¿Es exacta? ¿La audita y actualiza de manera regular? ¿Existen pruebas?

*El siguiente ejercicio ayudará a sus participantes a pensar de manera integral sobre qué datos recogen y conservan y cómo y dónde se almacenan. Esto les ayudará a saber no solo qué datos pueden necesitar, sino también qué tipo de protecciones deberían establecerse en relación con los distintos tipos de datos. También pondrá de relieve dónde pueden existir lagunas en la gestión adecuada de los datos. Al final del ejercicio los participantes deberán:*

*-conocer las distintas ubicaciones de sus datos y las formas que estos adoptan.*

*-pensar acerca de dónde y cómo se almacenan y quién tiene acceso a ellos.*

*-pensar en la importancia de los puntos anteriores en cuanto al derecho de supresión o en responder a una solicitud de acceso de un interesado.*

*-empezar a pensar acerca de los plazos de conservación.*

## Ejercicio 3: Asignación de datos

*Elija un conjunto de datos importantes para su centro (por ejemplo, información de clientes) y realice el siguiente ejercicio de asignación de datos respondiendo a las siguientes preguntas:*

- *¿Qué datos se recogen?*
- *¿El consentimiento se obtiene en el lugar de la recogida de datos?*
- *¿Dónde está almacenada la información? ¿En una base de datos, archivo de documentos, fichero de ordenador?*

- *¿Para qué se utilizan los datos?*
- *¿Quién puede acceder a ellos?*
- *¿Se ha compartido externamente?*
- *¿Cómo y cuándo se examinan, se completan o se actualizan los datos?*
- *¿Cuánto tiempo se conservan?*
- *¿Cuándo y cómo se eliminan?*

## Aprender de los demás: Las infracciones de las disposiciones sobre los datos en las noticias…

La entidad de beneficencia National Alzheimer's encontró graves fallas en la forma en que se manejan los datos personales sensibles, incluido el descubrimiento de voluntarios que utilizaban las direcciones de correo electrónico personales para recibir y compartir información sobre las personas que utilizan la entidad de beneficencia, almacenaban datos cifrados en sus ordenadores caseros y no mantenían bajo llave los registros de documentos. (ICO, 2016-01-07).

Clínica de salud multada con £180.000 (204.000 euros, 253.000 USD) por violación de la protección de datos al enviar accidentalmente un boletín con direcciones de correo electrónico de destinatarios en el campo «Para» en lugar de en el campo «CCO», lo que tuvo como consecuencia que revelara el estado VIH-seropositivo de dichos destinatarios. (ICO, 2016-05-09).

Memoria USB encontrada en el oeste de Londres con datos de seguridad aeroportuaria (Registro, 2017-10-30).

Detalles personales de hijos adoptivos, padres y trabajadores sociales enviados accidentalmente por correo electrónico a los invitados a una fiesta (Chronical Live, 2017-12-26).

Archivero repleto de documentos gubernamentales confidenciales termina en una tienda de segunda mano. (Guardian, 2018-02-02).

## Qué hacer y qué no hacer en relación con la confidencialidad

**Qué hacer**

- **Proteger** la confidencialidad de todas las personas identificables o la información confidencial con la que entre en contacto.

- **Ser consciente** de que cualquier información registrada acerca de una persona física debe protegerse, incluidas las notas y las agendas.
- **Despejar** su escritorio al final de cada día, manteniendo todos los registros portátiles que contengan información confidencial o sobre personas físicas identificables en lugares de archivo y almacenamiento reconocidos que estén bajo llave cuando sea imposible controlar o supervisar directamente el acceso a ellos.
- **Apagar** los ordenadores desde los que se pueda acceder a información sobre personas físicas identificables o a información comercial confidencial, o configurarlos en modo protegido por contraseña si abandona su escritorio durante cualquier periodo.
- **Asegurarse** de que no se le pueda escuchar cuando hable sobre asuntos confidenciales.
- **Desafiar y verificar**, cuando sea necesario, la identidad de cualquier persona que esté haciendo una solicitud de información confidencial o sobre una persona identificable y asegurarse de que tenga efectivamente la necesidad de conocerla.
- **Compartir** únicamente la información mínima necesaria.
- **Tener cuidado** al enviar faxes o correspondencia de correo electrónico y, cuando proceda, conservar un recibo de entrega o lectura.
- **Transferir** de forma segura información confidencial o sobre personas identificables, por ejemplo mediante el uso de un correo electrónico cifrado.
- **Pedir asesoramiento** si necesita compartir información sobre alguna persona identificable sin el consentimiento de esta última y registrar la decisión y cualquier medida que se tome.
- **Informar** de cualquier violación real o presunta de la confidencialidad.
- **Participar** en sesiones de inducción, sensibilización y formación sobre cuestiones relacionadas con la confidencialidad.

**Qué no hacer**

- **No compartir** contraseñas ni dejarlas tiradas en cualquier lugar para que otras personas las vean.
- **No compartir** información sin el consentimiento de la persona relacionada con ella, salvo si existen motivos legales para hacerlo.
- **No utilizar** información sobre personas identificables a menos que sea absolutamente necesario; anonimice la información siempre que sea posible.
- **No recoger, conservar ni tratar** más información que la que necesite; y no conservarla durante un tiempo mayor que el necesario.
- **No pensar** que los comentarios o las notas que haga solo serán para sus ojos; las personas físicas tienen derecho a acceder a la información conservada acerca de ellas mediante una solicitud de acceso del interesado.
- **No dejar** información desatendida en su escritorio.
- **NUNCA** dejar ficheros o información en el coche, en el autobús o cuando trabaje desde casa; asegúrese de que nadie pueda tener acceso a la información, salvo USTED.

*El siguiente ejercicio ayudará a los participantes a reflexionar de manera crítica sobre las prácticas actuales en su propia organización utilizando algunos dilemas comunes relacionados con la protección de datos. Deberá pedirles que piensen en todas las formas en que ellos y sus colegas manipulan, almacenan y transfieren información confidencial. Deben considerar las distintas prácticas de trabajo y el riesgo en relación con los datos que podría asociarse con ellas. Deben considerar posibles protecciones con el fin de minimizar el riesgo en relación con los datos. Si lo desea, puede pedir a los participantes que presenten algunas situaciones hipotéticas directamente relacionadas con su propia organización o práctica. Al final del ejercicio los participantes deberán:*

*-poder identificar los riesgos potenciales asociados con sus prácticas organizativas concretas.*

*-poder identificar las protecciones para minimizar los riesgos identificados anteriormente.*

## Ejercicio 4: Cosas en que pensar

*Piensen en lo que podrían hacer en caso de que se presenten las siguientes situaciones hipotéticas:*

1. *Ustedes tienen prisa de abandonar el centro. Quieren sus notas y documentos para comenzar el informe médico-legal, que piensan hacer en su portátil en el largo viaje en tren de regreso a casa.*

   *Consideren lo siguiente: ¿Cuáles son los posibles riesgos para la protección de datos?*

   *¿Cómo pueden minimizarlos?*

2. *Ustedes están trabajando en casa una noche en un borrador de un informe médico-legal que quieren que sea revisado al día siguiente. ¿Cómo pueden minimizar los riesgos para la protección de datos?*
3. *Encuentran algunas copias en papel de materiales sensibles de clientes en casa. ¿Cómo lidiarán con esto?*
4. *Se dan cuenta de que accidentalmente han enviado alguna información sobre un cliente a la dirección de correo electrónico personal de un colega. ¿Qué harán? ¿A quién le informarán del error?*

*El siguiente ejercicio ayudará a los participantes a entender cómo cumplir con una solicitud de acceso de un interesado según se dispone en el marco legislativo para la protección de datos expuesto anteriormente. Los participantes deberán remitirse al ejercicio de asignación de datos anterior (Ejercicio 3) para localizar toda la información que pudieran tener sobre una persona física, ya sea en copia en papel o en formato electrónico. Asimismo, deben examinar si alguno de los datos que conservan contiene información de terceros y cómo podrían actuar en lo que respecta a su supresión al dar respuesta a una solicitud de acceso de un interesado. También deben pensar en las posibles consecuencias para la persona física y asegurarse de tener la mayor claridad posible al respecto (por ejemplo, el envío de*

*datos sensibles sobre la salud por medio de un correo electrónico no seguro, etc.). Al final del ejercicio los participantes deberán saber:*
*-qué medidas tomar para lidiar con una solicitud de acceso del interesado.*

## Ejercicio 5: Cumplimiento con las solicitudes de acceso del interesado

*Ustedes reciben un correo electrónico de alguien que afirma que es el abogado de un cliente del centro y solicita una copia de los registros que conservan sobre él como una solicitud de acceso del interesado. ¿Cómo cumplen con esta solicitud? ¿Qué deben considerar para cumplir de manera adecuada y oportuna?*

*El siguiente ejercicio es hacer que los participantes piensen acerca de qué constituye una violación de la protección de datos o de la confidencialidad; y que traten de ver qué valor pueden asignar a la gravedad de esas violaciones. Al emitir sus juicios de valor, deben darle una explicación con respecto a cómo decidieron que un incidente era más grave o más importante que otro. También deberá pedirles que piensen en su propio contexto y que añadan sus propios incidentes a la lista. Cuando se producen violaciones, ¿cómo garantizar que esos incidentes les aporten experiencias de aprendizaje (y que no se repitan)? Al final del ejercicio los participantes deberán ser capaces de:*

*-identificar qué constituye una violación de la seguridad de los datos.*

*-identificar los distintos niveles de gravedad de las distintas violaciones de la seguridad de los datos.*

## Ejercicio 6: Clasifique las siguientes situaciones hipotéticas en orden de gravedad, de mayor a menor.

- *Ustedes encuentran copias de documentos dejados en una fotocopiadora en la oficina, entre ellos cartas y una lista de los problemas de salud mental y física de una persona.*
- *Un colega les dice que envió por correo electrónico información sobre un cliente, inclusive datos sensibles relativos a la salud, a una dirección de correo electrónico incorrecta.*
- *Un colega les dice que viajó con datos del cliente y que accidentalmente los dejó en el autobús o en el tren o en algún lugar que no recordaba.*
- *Un cliente muy preocupado acude a ustedes y les dice que su información y la información de un gran número de otros clientes fue encontrada en internet. Esta información incluye datos sensibles relativos a la salud.*
- *Ustedes descubren que alguien irrumpió en su oficina la noche anterior. Forzaron uno de los archivadores que contiene información sobre clientes y faltan documentos.*

- *Se percatan de que un colega ha enviado por correo electrónico un informe médico completo de un cliente a un determinado número de personas externas para que lo utilicen en un ejercicio de formación, sin el consentimiento por escrito del cliente.*
- *Un administrador ha enviado accidentalmente información de clientes (nombre, datos demográficos) al bufete de un abogado donde se publicaron los documentos accidentalmente junto con un informe médico-legal rellenado.*
- *Un informe médico-legal con datos personales muy sensibles se ha distribuido a los participantes en una formación sin la debida anonimización.*
- *Un administrador reveló por teléfono información acerca de un cliente sin haberse cerciorado debidamente si este último había concedido su consentimiento para que se revelara dicha información.*

# 4. Gestión responsable de datos: El panorama más allá de la simple protección de datos

*Hasta ahora, ha hablado de la protección de datos y de los tipos de datos que son pertinentes en determinados marcos legislativos. En esta sección, presentará la gestión responsable de datos a los participantes, que abarca un amplio conjunto de pensamientos, comportamientos, consideraciones aplicables a todo el ciclo de vida de los datos y no solo al contexto específico de los conjuntos de datos de personas identificables.*

*Objetivos de aprendizaje: al final de esta sección, los participantes:*

- *Escucharán una presentación sobre el concepto de «gestión responsable de datos».*
- *Comprenderán las implicaciones generales de la gestión ética y responsable de los datos en la gestión general de datos.*
- *Explorarán las posibles consecuencias de no poner en práctica la gestión responsable de datos.*

## ¿Qué es la gestión responsable de datos?

El deber colectivo de tener en cuenta consecuencias imprevistas al trabajar con datos:

1) dando prioridad a los derechos que tienen las personas físicas de dar su consentimiento, así como a la privacidad, la seguridad y la propiedad, cuando se utilizan datos en labores de cambio y asistencia social:

2) aplicando valores y prácticas de transparencia y apertura.

## ¿Qué es la gestión responsable de datos?

La gestión responsable de datos consiste en tratar con respeto los datos que recogemos y defender los derechos de las personas cuyos datos recogemos.

Consiste en ser responsable y consciente de los efectos que pueden tener en las personas todos los aspectos de la gestión de datos, entre ellos **la recogida, la manipulación, el almacenamiento** y **el uso**.

***Ser responsables con los datos de otras personas desde el punto de recogida hasta la publicación de informes.***

## Consideraciones en la gestión responsable de datos

Entre los elementos fundamentales de la práctica de la gestión responsable de datos figuran:

**Dinámicas de poder**: Las personas menos poderosas en cualquier situación son a menudo las primeras en ver las consecuencias imprevistas de los datos que se recogen acerca de ellas. Procesos como el codiseño o garantizar que personas de diversos estratos participen en la recogida de datos o en los procesos de análisis pueden servir para paliar dichas consecuencias.

Por ejemplo, en las crisis humanitarias, las personas cuyos datos se recogen tienen mucho menos poder que las que les solicitan sus datos. ¿Cómo podría esa asimetría de poder afectar la disposición de ellos para proporcionar sus datos?

**Diversidad y sesgo**: Considerar preguntas como «¿quién toma las decisiones? ¿qué perspectivas no se están considerando? ¿cómo podemos incluir una diversidad de pensamiento y enfoque?», puede sacar a relucir puntos ciegos y zonas donde la adición de otras voces sería útil.

Creemos que la diversidad, en todos sus tipos, fortalece nuestros proyectos y nuestro enfoque. Hemos visto proyectos, productos y organizaciones sufrir por tener personal o comunidades homogéneos y, a menudo, los efectos negativos de los datos los ven y los viven primero las comunidades marginadas. Necesitamos incluir esas voces y concebir maneras de mejorar como resultado de ello.

**Incógnitas**: No podemos ver el futuro, pero podemos diseñar pesos y contrapesos que nos alerten si ocurre algo inesperado.

A menudo, «pero no lo sabíamos» es lo primero que se escucha cuando hay consecuencias negativas imprevistas en un proyecto relacionado con datos. Es nuestra responsabilidad reflexionar acerca de cómo podemos diseñar rectificaciones para las consecuencias imprevistas especialmente importantes o impactantes.

**Principio de precaución**: El que podamos utilizar los datos de una forma determinada no necesariamente significa que debamos hacerlo. Si no podemos evaluar adecuadamente el riesgo y entender los daños a la hora de manipular datos, quizá deberíamos hacer una pausa durante un minuto y volver a evaluar lo que estamos haciendo y por qué.

La tecnología nos ofrece todo tipo de posibilidades. No todas ellas son acertadas; y no todas ellas van a tener buenos efectos en el mundo. Si trabajamos para que se produzcan

cambios en la sociedad, nuestra prioridad es respetar y proteger los derechos de las personas, y eso nos obliga a reflexionar sobre nuestras propias acciones.

**Innovación reflexiva**: Para que las nuevas ideas tengan la mejor oportunidad posible de éxito —y para que todos se beneficien de esas nuevas ideas y proyectos—, la innovación debe abordarse con cuidado y ponderación, no solo con celeridad.

La innovación consiste en la búsqueda de soluciones mejores y más eficaces para satisfacer mejor las necesidades. Para ello, en primer lugar debemos reservar un tiempo para pensar acerca de cuáles son esas necesidades, quizás a través de investigaciones, quizás de otras maneras. Debemos entonces pensar en qué posibles soluciones podrían satisfacer esas necesidades y tener efectos positivos cruciales (sin efectos secundarios negativos imprevistos) en la gente que estamos tratando de apoyar en el largo plazo.

**Exigirnos normas más rigurosas**: En muchos casos, los marcos jurídicos y normativos aún no consideran los efectos reales de los datos y la tecnología. ¿Cómo podemos esforzarnos para contar con normas más estrictas y predicar con el ejemplo?

Trabajar en el cambio y la promoción social significa que nos orientamos por un determinado conjunto de ideales. El beneficio no es nuestro objetivo; el cambio social positivo sí lo es. En muchas zonas del mundo, los marcos regulatorios presentan lagunas que permiten el desarrollo de proyectos que, tras una seria reflexión, pueden considerarse abusivos. Los países tienen distintos niveles de protección legal en lo que respecta a la privacidad, como el inminente Reglamento General de Protección de Datos de la Unión Europea, que protege firmemente esos derechos.

**Desarrollar mejores comportamientos**: No existe una talla única para la gestión responsable de datos. La cultura, el contexto y los comportamientos existentes cambian las implicaciones y las formas en que se utilizan los datos.

La gestión responsable de datos no es una práctica prescriptiva; lamentablemente no existen listas de comprobación que marcar para ser considerado «responsable». En buena medida se trata de la creación de enfoques mejor fundamentados para trabajar con los datos, que podrían incluir el examen periódico de las decisiones tomadas, teniendo en cuenta los nuevos elementos de información que vayan surgiendo. La puesta en práctica de la gestión responsable de datos no es solo una tarea para quienes manejan los datos directamente; es una cuestión operativa sobre la que todos, desde la alta dirección hasta el personal, deben reflexionar.

### *Si se tratara de usted y de sus datos, ¿cómo le gustaría que lo trataran o respetaran o que mantuvieran sus datos protegidos?*

***Confidencialidad***: El acceso a los datos estará restringido a aquellas personas que estén debidamente facultadas para ello.

***Integridad***: La información deberá ser completa y exacta. Todos los sistemas y activos deberán funcionar como se espera de ellos.

***Disponibilidad***: La información deberá estar disponible y entregarse a la persona adecuada, en el momento justo y cuando sea necesario.

*Pida a los participantes que consideren la siguiente situación hipotética, que sirve para poner de relieve algunas cuestiones en torno a la integridad y la* confidencialidad *de los datos. Al final del ejercicio los participantes deberán ser capaces de:*

*-identificar estas cuestiones de integridad y confidencialidad de los datos.*

*-prever qué consecuencias podría haber para el cliente.*

### Ejercicio 7: Integridad y confidencialidad de los datos

*Situación hipotética*
*JP es un cliente del centro y está asistiendo a citas regulares para recibir terapia psicológica debido a las torturas de que fue víctima cuando estuvo detenido por la policía estatal.*
*Debido a un error de introducción de datos, un administrador llama por error al número de teléfono de su trabajo en lugar de a su número personal y como JP se encuentra en una reunión, uno de sus colegas descuelga el teléfono. Pensando que JP ha contestado, el administrador le pregunta si puede cambiar su cita para una fecha posterior.*
*Dado que el administrador revela de dónde proviene la llamada, es de inmediato evidente para el colega de JP que éste está recibiendo tratamiento en el centro y, aún peor, revela esta información a sus colegas.*

*Preguntas:*

- *¿Qué lecciones pueden aprenderse de la situación hipotética anterior?*
- *¿Cuáles son las posibles consecuencias para JP?*

*Pistas:*

- *En la casilla del número de trabajo debe figurar el número personal.*
- *La confidencialidad es violada cuando el administrador le revela a una persona distinta de JP la información personal de este último.*

## 5. El ciclo de vida de los datos

*En esta sección, presentará el ciclo de vida de los datos a los participantes y les pedirá que piensen acerca de la forma en que encajan en cada paso las consideraciones de gestión responsable de datos. Les pedirá a los participantes que realicen algunos ejercicios prácticos con el fin de practicar las técnicas de gestión responsable de datos. Los participantes deben pensar acerca de los diferentes tipos de riesgos y amenazas que habrán de tener en cuenta en las diferentes etapas del ciclo de vida de la gestión de datos.*

*Objetivos de aprendizaje: al final de esta sección, los usuarios:*

- *Comprenderán el ciclo de vida de los datos y cómo encajan en cada paso las consideraciones de la gestión responsable de datos.*
- *Entenderán cómo evaluar el riesgo cuando se trata de la gestión de datos y realizarán una evaluación de riesgo considerando las protecciones posibles.*

- *Entenderán cómo tomar en consideración la privacidad de las personas a la hora de considerar la gestión de datos y en qué consiste la evaluación de impacto relativa a la privacidad.*

## Comprender el ciclo de vida de los datos

El ciclo de vida de los datos es la secuencia de etapas por la pasa que una determinada unidad de datos, desde su generación o recogida inicial hasta su eventual archivo o supresión. Se han identificado 6 o más etapas en el ciclo de vida habitual de los datos, que abarca la **recogida**, la **manipulación**, **el almacenamiento** y el **uso** de los datos.

**I. Recogida**

1. Planificación: Traten de pensar acerca de cuáles son los resultados que están intentando alcanzar y qué tipos de información necesitarán recoger para llegar allí.
2. Evaluación del riesgo: ¿Están haciendo la pregunta porque mejorará su conjunto de datos o por algún otro motivo?
3. Formación del personal y de otras personas encargadas de recoger los datos: asegurarse de que el personal entienda y aplique las técnicas de manipulación responsable de datos.
4. Consentimiento: Se considera una «regla de oro» de buena práctica garantizar que exista un consentimiento informado correcto cuando se obtienen y utilizan datos personales.

**II. Manipulación y III. Almacenamiento**

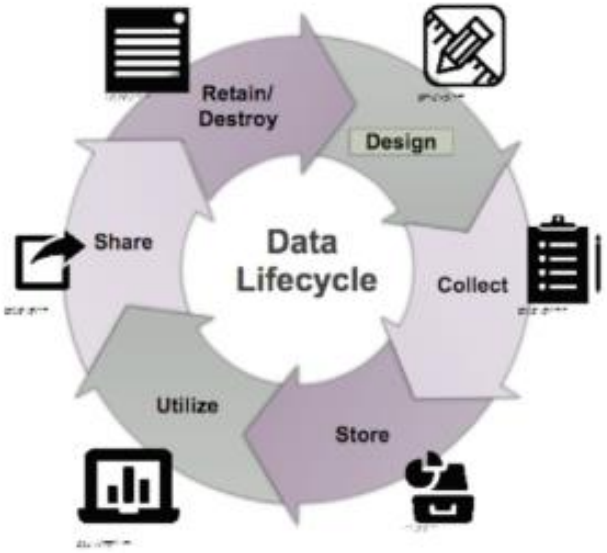
5. Gestión: ¿Cómo recogerá, almacenará, utilizará, compartirá los datos? ¿Cómo se cerciorará de que sus datos sean exactos? ¿Es necesario que establezca medidas para revisar, limpiar, purgar los datos periódicamente?

**IV. Uso**

6. Uso: ¿Cómo utilizará lo que se ha recopilado?
7. Comentarios: Un aspecto fundamental de la gestión ética de los datos es garantizar que quienes han confiado en proporcionarle sus datos personales reciban comentarios siempre que sea posible sobre las cosas buenas que se han obtenido mediante la utilización de sus datos.

**Manipulación y almacenamiento**

8. Conservación y destrucción: ¿Cuánto tiempo debo mantener mis datos? ¿Debo mantener todos los datos o sólo conservar algunos? ¿Puedo anonimizarlos?




# I. Recogida

## Planificación: Evaluaciones de riesgos, evaluaciones de impacto en lo relativo a la privacidad, consentimiento informado, formación.

Paso 1: Elaborar un **plan**. Definan con claridad la finalidad de la recogida de datos. Los beneficios que se esperan de la recogida de datos deben ser proporcionales a los riesgos. Ustedes deben orientarse por los intereses y el bienestar de las personas acerca de las cuales están recogiendo los datos. No recojan más datos que los necesarios. Planifiquen la anonimización desde el diseño, siempre que sea posible. Planifiquen cómo obtendrán el consentimiento informado antes de comenzar. Verifiquen la presencia de cualquier sesgo en sus métodos de recogida. ¿Cómo verificarán la exactitud y la depuración de sus datos?

Paso 2: Realicen una **evaluación de riesgos.** La recogida de datos puede poner a las personas en riesgo. Evalúen los riesgos y adopten medidas para evitar consecuencias negativas, por ejemplo, garantizando la seguridad de los datos y la confidencialidad.

El riesgo relativo a la privacidad es el riesgo de causar daños derivados de una intromisión en la privacidad. Algunas de las formas en que puede presentarse este riesgo es si la información personal:

- Es inexacta, insuficiente o está desactualizada;
- Es excesiva o no pertinente;
- Se conserva durante demasiado tiempo;
- Se revela a personas a quienes la persona no quiere que se les revele;
- Se utiliza de formas que son inaceptables o imprevistas para la persona en cuestión; o

- No se conserva de forma segura;

El daño puede presentarse de diversas formas. A veces será tangible y cuantificable, por ejemplo, pérdida financiera o pérdida de un empleo. En otras ocasiones será menos definido, por ejemplo, daños a las relaciones personales y a la situación social derivados de la revelación de información confidencial o sensible.

Con una evaluación de impacto relativa a la privacidad se intentan evaluar —e informar al respecto— los posibles impactos a la privacidad de una persona cuando las organizaciones tratan datos personales.

Qué debe considerarse cuando se realizan evaluaciones de impacto relativas a la privacidad:

- ¿Por qué motivo se recoge información de una persona identificable?
- ¿Las personas de las que recojo los datos ejercen su capacidad de elección y dan su consentimiento para su tratamiento?
- ¿Tengo establecidas políticas que rijan el uso y el tratamiento de información de personas identificables? ¿Estas políticas son sólidas y adecuadas para la finalidad prevista?
- ¿El personal recibe apoyo y formación de manera regular?
- ¿Existen registros de auditoría claros del lugar en que se almacenan y transmiten los datos?
- ¿Se han establecido protocolos claros relativos al intercambio de información?

*El siguiente ejercicio ayudará a los participantes a pensar en todos los aspectos de la gestión de datos antes de iniciar un nuevo proyecto o servicio. Los participantes deberán elegir claramente un nuevo proyecto o proceso y examinar todos los aspectos de la gestión responsable de datos (GRD) en su plan. Este ejercicio deberá resaltar la importancia de pensar en la GRD antes de iniciar cualquier nuevo proyecto, proceso o servicio, de manera que se puedan incorporar y comunicar desde el principio los principios de dicha gestión.*

*Los participantes deberán empezar a pensar acerca de la finalidad del ciclo de datos desde el principio, así como considerar qué tipo de preguntas están tratando de responder desde el principio, por ejemplo, texto libre frente a datos clasificados, y los pros y los contras de cada uno. Al final del ejercicio los participantes deberán ser capaces de:*

*-identificar las prácticas de GRD durante el ciclo de vida de los datos desde el principio hasta el final.*

## Ejercicio 8: Elaborar un plan

*Pida a los participantes que se organicen en parejas o en pequeños grupos y que elaboren un plan para un nuevo proyecto que llevará a cabo su organización o un servicio que esta prestará. Asegúrese de que aborden lo siguiente en sus planes:*

- *¿Cuál es el proyecto o el servicio que están tratando de lograr?*
- *¿Cuál es la finalidad de la recogida de los datos y qué harán con ellos?*
- *¿Qué métodos aplicarán para recoger los datos?*
- *¿Cómo obtendrán el consentimiento informado?*
- *¿Cómo capacitarán a su personal?*
- *¿Cuáles son los riesgos y cómo lidiarán con ellos?*
- *¿Qué forma adoptarán los datos? ¿Clasificados, no clasificados, texto libre?*
- *¿En qué forma deben estar los datos para cumplir con el tipo de análisis que desean realizar, si procede? ¿Deben cumplir con otros conjuntos de datos? (por ejemplo, acuerdo de categorías o grupos)*
- *¿Cómo lidiarán con las respuestas a determinados datos clasificados cuando dichas respuestas no existan (por ejemplo, alguien responde «ninguno» a la pregunta «¿Cuál es su género?» y las respuestas en su sistema son «masculino», «femenino»)?*
- *¿Qué protecciones necesitarán establecer con respecto al acceso, la transferencia, el almacenamiento o el intercambio de datos?*
- *¿Cuánto tiempo conservarán o archivarán los datos y cuándo los eliminarán? ¿Cuentan con una forma de anonimizar los datos antes de archivarlos?*

*El siguiente ejercicio ayudará a los participantes a reflexionar sobre prácticamente todos los riesgos vinculados con los diversos tipos de manipulación de datos y a establecer protecciones para abordar esos riesgos. Al final del ejercicio los participantes deberán ser capaces de:*

*- sopesar y conciliar el riesgo de recoger los datos y los beneficios de utilizar esos datos.*

## Ejercicio 9: Evaluación del riesgo de manipulación de datos

*Pida a los participantes que rellenen el siguiente cuadro, que evalúen los riesgos y que asignen una puntuación de riesgo a cada uno de ellos. Pídales que indiquen los controles que podrían tener establecidos a la fecha y que traten de determinar qué nuevos controles podrían necesitar para que también los establezcan. El cuadro contiene algunas posibles sugerencias para ellos. Añada otros riesgos en la evaluación a medida que vayan determinándolos.*

| Identificación de riesgos e impacto(s) posible(s) | Tipo de riesgo | Puntuación del riesgo antes del control:<br>Probabilidad x Impacto (min. 0, máx. 25) | Controles / garantías existentes | Puntuación del riesgo después del control:<br>P x I | Otras acciones planificadas |
|---|---|---|---|---|---|
| Visualización / acceso no autorizados / pérdida de documentos impresos en tránsito | | | | | |
| Personal / voluntarios con documentación en casa / lugares externos | | | | | |
| Correos electrónicos enviados desde direcciones de correo electrónico personales | | | | | |
| Documentos enviados por correo electrónico al destinatario equivocado | | | | | |
| Pérdida o robo de ordenadores portátiles o unidades de USB | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| Datos inexactos o incompletos | | | | | |
| Datos duplicados | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Paso 3: **Impartir formación** a su personal. Asegúrese de que su personal conozca y entienda la protección de datos y las consideraciones relacionadas con la gestión responsable de datos. Asegúrese de que se realicen evaluaciones de riesgos. Asegúrese de que sepan cómo obtener el consentimiento informado. Asegúrese de que reciban formación en prácticas óptimas de seguridad de datos.

Paso 4: Obtener el **consentimiento informado.** Comunique a los entrevistados la forma en que utilizará sus datos y por qué los necesita.

- ➔ **Explicar**. Explique claramente a las personas cómo se utilizará la información personal acerca de ellas e indíqueles dónde encontrar más información al respecto, por ejemplo, en el sitio web de su organización, en un folleto o cartel.
- ➔ **Ofrecer opciones**. Ofrézcales a las personas una opción acerca de cómo se utilizará su información y dígales si esa elección afectará a los servicios que se les ofrecen.
- ➔ **Satisfacer las expectativas**. Utilice la información personal solo de la forma en que las personas lo esperarían de manera razonable.

*En este ejercicio, los participantes reflexionarán acerca de cómo podrían obtener el consentimiento informado en su propio contexto. Deben pensar en todas las formas en que utilizan los datos de los clientes y asegurarse de que éstas se incluyan en cualquier formulario de consentimiento. Los participantes deberán considerar la posibilidad de solicitar el consentimiento a personas vulnerables que necesiten que se les expliquen las cosas de maneras diferentes, que no siempre entiendan plenamente qué es el consentimiento, y que posteriormente puedan retirar el consentimiento ya otorgado. Al final del ejercicio los participantes deberán ser capaces de:*

*-asegurarse de que los formularios de consentimiento reflejen la forma en que su organización utiliza (y piensa utilizar) la información de los clientes.*

*-tener en cuenta las cuestiones relativas al consentimiento de personas vulnerables*

.

## Ejercicio 10: Consentimiento informado

*a) Teniendo presente sus propios servicios y su contexto, elaboren un formulario de consentimiento que abarque los distintos usos que hace su organización de los datos. Asegúrense de que su formulario sea claro y conciso y que refleje con exactitud las opciones que puedan ofrecerse.*

*Si lo desean, pueden también asegurarse de que su formulario indique los acuerdos de intercambio de datos comunes cuando su servicio comparte datos con otras entidades (p. ej., otros servicios de salud, etc.).*

*b) En parejas (o con un asociado), practiquen la elaboración del formulario de consentimiento y la obtención del consentimiento informado.*

# II. Manipulación y almacenamiento

Paso 5: **Gestionar sus datos**

➔ Asegurar la calidad de los datos: Depurar, proteger, mejorar.

Consideren lo que necesitarán establecer para asegurar la integridad de sus datos y registros: que estén depurados y sin duplicaciones ni errores.

***Cosas en que pensar:***

*¿Cuáles son las posibles consecuencias de tener datos no depurados? Piensen concretamente tanto en la gestión cotidiana de un servicio (véase el ejemplo anterior relacionado con JP) como en cualquier tipo de análisis o toma de decisiones que pueda derivarse de los datos del participante. ¿Qué tipo de información o conclusiones ellos (u otras personas) extraen de estos datos? ¿Qué políticas o procesos podrían necesitar establecer para garantizar la buena calidad de los datos?*

*En el siguiente ejercicio, los participantes reflexionarán sobre la utilidad de contar con datos depurados y estandarizados, así como en los posibles riesgos que implican unos datos de mala calidad. Aprenderán a estandarizar un conjunto pequeño y la forma en que esto contribuye a la depuración de los datos y a reducir errores en el análisis. Al final del ejercicio los participantes deberán ser capaces de:*

*-depurar los datos.*

*-comprender cómo la depuración y la estandarización de los datos contribuye a la integridad de estos.*

## Ejercicio 11: Depuración y estandarización de datos

*Pida a los participantes que vean el siguiente conjunto de datos y sugiera formas de depurarlo o estandarizarlo.*

| | | | |
|---|---|---|---|
| Jane Doe | Nueva York | Terapia clínica | 15/01/1978 |
| Ahmid Assan | N.Y. | Terapia | 15 de enero de 1978 |
| Georgeau Constantine | ny | clínica | 15/01/1978 |

- ➔ Transferencia: Tengan cuidado al utilizar dispositivos portátiles o al trasladar registros impresos. Cifren los registros digitales. Restrinjan el acceso. Asegúrense de que los dispositivos estén cifrados. Tengan especial cuidado al trasladar registros en papel que estén en riesgo de pérdida o robo.
- ➔ Acceso: Asegúrense de que el acceso esté restringido según el principio de la «necesidad de conocimiento». Restrinjan el acceso a los registros y sistemas. Asegúrense de que los registros impresos estén bajo llave en todo momento y que el acceso esté controlado.
- ➔ Almacenar: Asegúrense de conocer y comprender dónde se almacena su información; y
- ➔ Compartir: ¿Necesitarán compartir todos o parte de sus datos? Por ejemplo, registros individuales para dar apoyo a un cliente, o bien mayores conjuntos de datos con un asociado de investigación?

*Los participantes aprenderán a elaborar un acuerdo básico de intercambio de datos, teniendo en cuenta las cuestiones relacionadas con la protección de los datos y la posible utilidad de compartirlos. Los participantes deberán considerar si las técnicas de anonimización pueden ser adecuadas en el contexto del ejemplo que hayan elegido. Al final del ejercicio los participantes deberán ser capaces de:*

*-entender las cuestiones relativas a la protección de datos a la hora de compartir datos.*

*-crear un acuerdo de intercambio de datos sencillo.*

## Ejercicio 12: Acuerdo de intercambio de datos

*Pida a los participantes que piensen en los asociados que trabajan con ellos y en qué circunstancias pueden necesitar compartir datos. Elaborar un modelo de acuerdo de intercambio de datos para ello.*

*El objetivo de las siguientes situaciones hipotéticas es que los participantes piensen en cómo podrían conciliar las necesidades del servicio y los principios de protección de datos. Al final del ejercicio los participantes deberán ser capaces de:*

*-conciliar posibles intereses en conflicto al considerar la gestión responsable de datos.*

## Ejercicio 13: Cosas en que pensar

*¿Cómo responderían ante las siguientes situaciones hipotéticas o cómo asesorarían a sus compañeros de trabajo para que respondan a ellas:*

- *Están recogiendo información de un sobreviviente y este les pregunta qué va a ocurrir con la información que les está dando.*
- *Están recogiendo información histórica de un sobreviviente con ayuda de un traductor, y aunque la respuesta a una pregunta del sobreviviente fue muy larga y emotiva, resulta evidente que el traductor hizo un resumen de lo que dijo.*
- *Una organización asociada quiere llevar a cabo un proyecto conjunto que implicaría la necesidad de un intercambio de datos. ¿En qué necesitarían pensar o qué deberían establecer al considerar esto?*
- *Un nuevo compañero de trabajo se incorpora en su organización y le pregunta cuál es su política en torno al consentimiento o la denegación de los clientes para que utilicen sus datos en determinadas actividades. ¿Qué le dicen?*

# III. Uso

Paso 6: ¡**Use** sus datos! Podría ser en actividades de cabildeo, promoción o aprendizaje aplicado a sus propios servicios. Piensen en quién está representado en los datos. ¿Han considerado algún sesgo? ¿Equilibrio de género? ¿Confían en la calidad de los datos? ¿En la calidad del análisis?

Paso 7: Dén **retroalimentación**. Es una buena práctica hacer participar a las personas cuyos datos recogieron en el uso que hagan de estos. Por ejemplo, si han utilizado los datos para escribir un informe con fines de promoción, es una buena práctica compartir ese informe con los entrevistados siempre que sea posible.

Paso 8: **Conservación y destrucción**. Asegúrense de tener establecidas políticas de conservación y destrucción adecuadas. ¿Necesitan conservar los datos en su forma actual? ¿Tienen que conservar datos personales? ¿Hay una manera de conservar solo datos agregados? ¿O de anonimizarlos? En caso contrario, ¿tienen la capacidad de recuperar registros individuales para destruirlos (véase *supra* «Derecho de supresión» bajo RGPD)? A la hora de optar por eliminar, asegúrense de que la supresión sea permanente y que también se eliminen todas las copias o versiones.

## *La gestión de datos eficaz y responsable abarca todo el ciclo de vida de los datos.*

## Conclusión: ¿por dónde empezar? Cosas que pueden empezar a hacer ahora

- Crear conciencia entre sus compañeros de trabajo, contratistas y asociados en lo que respecta a la seguridad en la manipulación de datos, especialmente con los funcionarios de mayor jerarquía de su organización.

- Impartan formación y comuníquense con su personal en torno a la gestión responsable de datos y a las medidas de seguridad relativas a los datos, incluidas las políticas para garantizar que se bloquee el acceso cuando el personal abandone la organización.
- Asegúrense de que disponen de sólidas políticas y procedimientos relativos a la seguridad en la gestión y protección de datos personales. Políticas: Protección de datos, seguridad de la información, confidencialidad, intercambio de datos, informes de incidencias (de infracción), recuperación, divulgación.
- Asegúrense de contar con una estructura de rendición de cuentas clara en lo relativo a la manipulación los datos.
- Garanticen la transparencia en la manipulación de los datos y asegúrense de que a aquellas personas cuyos datos personales manipulan se les comunique de manera clara la forma en que se utilizarán.
- Establezcan un sistema de evaluación de riesgos y de evaluaciones de impacto relativas a la privacidad, siempre indagando sobre nuevas formas de recogida de datos o de hacerlo de manera diferente. Un plan puede ser sumamente útil para ayudarles a pensar en los riesgos y en las posibles consecuencias que se enfrentarían en caso de una fuga de datos.
- Utilicen un enfoque basado en los riesgos y piensen en qué podría marchar mal con el fin de intentar establecer medidas preventivas para reducir el riesgo.
- Deber de sinceridad: Estén dispuesto a revelar en caso de que se produzcan violaciones o pérdidas involuntarias o corrupción de datos.
- Asegúrense de que disponen de contratos sólidos que prevean asuntos relativos al intercambio de datos o a la subcontratación de algún tratamiento de datos.
- Revisen la seguridad de la TI y asegúrense de que se tengan establecidas medidas adecuadas de cifrado, copias de seguridad, actualizaciones, uso de dispositivos personales (*BYOD*: traiga su propio dispositivo), etc.
- Asegúrense de contar con un plan de respuesta a incidentes en caso de violación relativa a los datos.

# 6. Glosario

**Agregado**: Forma de agrupar en una clase o en un clúster con fines de análisis o anonimización a un nivel superior.

**Violación de la seguridad de los datos:** Incidente de seguridad en el que una persona no autorizada copia, transmite, visualiza, roba o utiliza **datos** sensibles, protegidos o confidenciales.

**Cumplimiento relativo a los datos**: La integridad de un conjunto de datos.

**Depuración de datos**: Proceso mediante el cual se detectan y corrigen (o eliminan) registros corrompidos o inexactos de un conjunto de registros, cuadro o base de datos; asimismo, se refiere a la identificación de partes incompletas, incorrectas, inexactas o irrelevantes de los datos para luego sustituir, modificar o eliminar aquellos datos no depurados o toscos.

**Responsable del tratamiento**: Persona física o jurídica que determina los fines y la forma en que se tratan o se tratarán los datos personales.

**Gobernanza de los datos**: Proceso(s) que define una organización para asegurarse de que existan datos de alta calidad a lo largo de su ciclo de vida.

**Higiene de los datos**: Procesos colectivos aplicados para garantizar la depuración de los datos. Los datos se consideran depurados si están relativamente libres de errores. La existencia de datos no depurados puede obedecer a una serie de factores, entre ellos registros duplicados o datos incompletos o no actualizados, así como al análisis inadecuado de campos de registro de sistemas dispares.

**Ciclo de vida de los datos**: Flujo de información a lo largo de un sistema, desde la creación y el almacenamiento a la eliminación.

**Encargado del tratamiento**: Persona física o jurídica que trata datos personales por cuenta del responsable del tratamiento.

**Responsable(s) de la protección de datos**: Persona(s) responsable(s) de garantizar que una o diversas organizaciones cumplan con la legislación relativa a la protección de datos y a menudo con sus propias políticas internas relativas a la protección de datos.

**Conjunto de datos**: Serie de datos relacionados.

**Acuerdo de intercambio de datos**: Acuerdo o marco de referencia relativo al intercambio de datos en el que se establece cómo se transmitirán, almacenarán y utilizarán los datos.

**Estandarización de datos**: Proceso crucial mediante el cual los datos se organizan en un formato común que permite la colaboración entre investigadores, el análisis a gran escala y el intercambio de herramientas y metodologías complejas.

**Interesado**: Persona concernida por los datos de carácter personal.

**Cifrado**: Proceso que consiste en codificar mensajes o elementos de información de forma tal que solo puedan leerlos las personas autorizadas. El cifrado en sí no evita la interceptación, pero impide visualizar el contenido del mensaje por el interceptador.

**RGPD** – Reglamento General de Protección de Datos: Nueva legislación sobre protección de datos de los interesados en la Unión Europea.

**Comisario de Información**: Autoridad responsable de la supervisión y aplicación de la legislación de protección de datos en el Reino Unido.

**Ética de la información**: «rama de la ética que se centra en la relación entre la creación, organización, difusión y uso de la información, y las normas éticas y los códigos morales que rigen la conducta humana en la sociedad».

**Gobernanza de la información**: Gestión de la información en una organización. La gobernanza de la información concilia el uso y la seguridad de la información.

**Consentimiento informado**: Acuerdo voluntario y libre basado en una clara apreciación y comprensión de los hechos, las implicaciones y las posibles consecuencias futuras de una acción.

**Datos personales**: Datos relativos a una persona viva susceptible de ser identificada a partir de ellos o de los datos y otros elementos de información que se encuentren en poder del responsable de los datos o que sea probable que vayan a estar en poder de este último.

**Phishing** (**suplantación de identidad**): Intento de obtener información sensible, como nombres de usuario, contraseñas o datos de tarjetas de crédito (y a veces, de forma indirecta, dinero) a menudo por motivos maliciosos, haciéndose pasar por una entidad de confianza en una comunicación electrónica.

**Tratamiento**: Recogida, modificación, manipulación, almacenamiento o revelación de información personal.

**Evaluación de impacto en la privacidad**: Evaluación realizada para determinar el impacto de cualquier nuevo tratamiento en la privacidad de los interesados. Es una herramienta que se utiliza para identificar y reducir los riesgos relativos a la privacidad.

**Seudónimo**: Nombre ficticio o alias.

**Gestión de registros**: Campo de la gestión responsable que se ocupa del control eficiente y sistemático de la creación, recepción, mantenimiento, uso y eliminación de registros. Incluye la identificación, clasificación, almacenamiento, protección, recuperación, seguimiento y destrucción o conservación permanente de los registros.

**Supresión**: Censura u ocultamiento de parte de un texto o información con fines legales, de seguridad, privacidad o anonimización.

**Datos personales sensibles**: Término relativo a los datos sobre:

- El origen racial o étnico.
- Las afiliaciones políticas.
- La religión o creencias similares.
- La afiliación sindical.
- La salud física o mental.
- La sexualidad.
- Los antecedentes penales o los procedimientos jurídicos.

**Solicitud de acceso del interesado**: Toda solicitud (por escrito) por un interesado relativa a la información personal que conserve una organización sobre él o ella.

# 7. Referencias / Otros recursos


- Care Quality Commission. *Datos seguros, atención segura*. https://www.cqc.org.uk/sites/default/files/20160701%20Data%20security%20review%20FINAL%20for%20web.pdf
- Comisario de Protección de Datos de Irlanda. El *RGPD y usted* http://gdprandyou.ie/
- DLA Piper, leyes de protección de datos del mundo. https://www.dlapiperdataprotection.com/index.html?t=world-map&c=DK
- Reglamento General de Protección de Datos https://www.eugdpr.org/
- Geraghty, R. (2016). *Anonimización e investigación social*. https://www.slideshare.net/ISSDA/anonymisation-and-social-research?qid=fa5a5338-8766-4b0b-9bf6-105f852d5932&v=&b=&from_search=1
- Oficina del Comisionado de Información https://ico.org.uk/
- Oficina del Comisionado de Información (2017). *Prepararse para el Reglamento General de Protección de Datos (RGPD): 12 pasos que dar ahora*. https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
- Oficina del Comisionado de Información (2017). *Código de Práctica de Acceso de los Interesados: Atención de solicitudes de acceso a información personal de particulares*. https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf
- Oficina del Comisionado de Información. *Traiga su propio dispositivo (BYOD)*. https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf
- ICRC. https://www.icrc.org/eng/assets/files/other/icrc-002-0999.pdf*Normas profesionales para el trabajo de protección*. https://www.icrc.org/eng/assets/files/other/icrc-002-0999.pdf
- Guardián Nacional de Datos para la Salud y la Atención. *Revisión de seguridad de los datos, consentimiento y exclusión voluntaria (*opt-out*)*. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF
- NHS Digital. *Sensibilización en materia de seguridad de datos Nivel 1*. https://www.igt.hscic.gov.uk/
- NHS, Inglaterra. *Information Governance Handbook* (Manual de gobernanza de la información).
- Foro de Gestión Responsable de Datos: https://responsibledata.io/
- Servicio de Datos del Reino Unido. *Anonimización.* https://www.ukdataservice.ac.uk/manage-data/legal-ethical/anonymisation

Apéndice A

# Plantilla del Programa de Formación

Objetivos de formación: Desarrollar habilidades y conocimientos sobre gestión responsable de datos (recogida, manipulación, almacenamiento, utilización) y desarrollar habilidades para formar a otros.

**Día 1**

09:00-10:30 (1,5 h)

Introducción a la gestión responsable de datos

- ¿Por qué es necesario proteger?
- Piensen en cómo querrían que se manipularan sus propios datos.

¿Qué datos?

- Datos personales, datos sensibles

  → Ejercicio: Identificar y clasificar los datos personales, sensibles confidenciales
- anonimización y seudonimización
- agregación

  → Ejercicio: Enumeren conjuntos de datos que suelen ser objeto de tratamiento en su propio contexto; clasificación de conjuntos de datos propios; comiencen a pensar en el intercambio de información.

10:30: PAUSA [15]

10:45-12:30 (1,75 h)

Introducción al marco legislativo de la UE / RGPD

- RGPD: El ordenamiento jurídico de la UE. El contexto general y el ordenamiento jurídico: Reglamento General de Protección de Datos (RGPD) Europeo
- Derechos de los interesados; obligaciones de los responsables del tratamiento de datos

  → Ejercicio: Asignación de datos

  →Ejercicio: Situaciones hipotéticas de protección de datos y hacer que las personas piensen en la forma en que responderían. Hacer que las personas piensen de posibles situaciones hipotéticas en su propio contexto.

12:30: ALMUERZO [60]

13:30-15:00 (1,5 h)

RGPD (continuación)

- Solicitudes de acceso de los interesados: qué son y cómo cumplir con ellas

  → Ejercicio: Cumplimiento de las solicitudes de acceso los interesados, información de terceros, supresión

  → Ejercicio: Situaciones hipotéticas de protección de datos

15:00: PAUSA (15 m)

15:15-16:30 (1,25 h)

Continuar con los ejercicios, haciendo que los participantes traten de presentar conjuntos de datos de la vida real relacionados con su trabajo cotidiano, así como situaciones hipotéticas reales relacionadas con su trabajo cotidiano

Piensen acerca de la toma de decisiones basada en el riesgo

16:30: Recapitulación del día y anuncio de los temas del día siguiente

**Día 2**

9:00-10:30 (1,5 h)

Recapitulación de los temas del día anterior

Introducción a la gestión responsable de datos

- ¿Qué es la GRD?
- ¿Por qué queremos poner en práctica una GRD regida por principios éticos?
- Consideraciones en torno a la GRD
- Confidencialidad, integridad, disponibilidad

  → Ejercicio: situación hipotética y debate

10:30: PAUSA [15]

10:45-12:15 (1,5 h)

El ciclo de vida de los datos: Descripción general del ciclo de vida de los datos

- Un ciclo de vida común: pasos en el ciclo de vida de los datos y riesgos en las distintas etapas
- Recogida, almacenamiento, manipulación, uso: los 8 pasos en este marco
- I. Recogida: Recogida responsable de datos
  - Introducción a la planificación, cosas en que pensar cuando se planifica un nuevo proyecto o servicio que implique la recogida de datos, evaluaciones de impactos relativos a la privacidad, consentimiento informado, garantizar las competencias adecuadas entre los encargados de recoger datos, conjuntos de datos estandarizados

- Evaluación de riesgo en la GRD: estar preparados para las situaciones más desfavorables / aprender de otras personas

→ Ejercicio: Elaborar un plan: Piensen en una actividad de servicio básico o en un nuevo proyecto y en cómo podrían actuar al llevar a cabo una evaluación de impacto relativa a la privacidad en lo que respecta a los datos que están recogiendo. Recuerden pensar en las diferencias entre datos personales (DP) y datos no personales (DNP)

→ Ejercicio: Realicen una evaluación de riesgos

- Impartir formación a su personal
- Consentimiento: informado, adecuado, flexible. Consentimiento informado: qué es, qué aspecto tiene, cuál es la finalidad de la recogida, planificación para el retiro del consentimiento o si la persona cambia de parecer.

→ Ejercicio: Elaborar un formulario de consentimiento que se les presentará a las personas que acuden a sus servicios en el punto de acceso. Necesitan reflexionar en cómo transmitir el uso que le darán a la información y por qué la necesitan.

→ Ejercicio: Practiquen la obtención del consentimiento informado

12:15 - recapitulación y anuncio de los temas del día 3

**<u>Día 3</u>**

9:30-11:00 (1,5 h)

Recapitulación de los temas tratados hasta la fecha / Preguntas y respuestas

El ciclo de vida de datos (continuación)

- II. Manipulación y III. Almacenamiento
  - Gestión de datos. Garantizar la integridad de los datos, la calidad de los datos, la estandarización, la validez, la comparabilidad; cómo se relacionan estos temas con la ética en la gestión de datos. Establecer una infraestructura adecuada: acceso controlado, almacenamiento seguro (físico y electrónico), intercambio y transferencia de forma segura, anonimización, seudonimización. Cifrado. (Consultar Solicitud de acceso del interesado, Día 1).

  → Ejercicio: Depuración de datos

  - Gestión de datos (continuación)

  → Ejercicio: Acuerdos de intercambio de datos

  → Ejercicio: Situaciones hipotéticas / Cosas en que pensar

11:00: PAUSA

11:15-12:30 (1,25 h)

- IV. Uso responsable de los datos
    - Uso: Acción sobre →información→ y datos: cabildeo, promoción, evaluación de programas. Mejora de la calidad. Cambio. Consideración sobre cómo los datos pueden utilizarse de manera inadecuada

      ¿Para qué utilizan los datos? ¿Cómo pueden asegurarse de que no sean utilizados de manera inadecuada?
    - Retroalimentación: Proporcionar retroalimentación en la medida de lo posible, cerrar el ciclo y dar a conocer los resultados y el análisis a los titulares de los datos, mostrándoles qué sucedió y qué se logró.

      → Ejercicio: ¿Cómo pueden proporcionar retroalimentación a las personas que utilizan sus servicios sobre lo que han hecho con sus datos? (Piensen en informar sobre el intercambio de datos o sobre los resultados de una labor de cabildeo: posibles medios de comunicación: grupos / sitio web)

ALMUERZO (60 m)

13:30-14:30 (1 h)

- Conservación y eliminación. - Políticas de conservación y procesos adecuados establecidos. «La sombra de los datos»: conocer la ubicación de sus datos: localmente, en redes, en la nube. Relacionar la conservación con la Solicitud de acceso del interesado

  → Ejercicio: Elaborar un programa de conservación para los diversos tipos de datos que estén en su poder

- Incorporación de la GRD en su organización

  → Ejercicio: Elaborar un plan de acción sobre qué harán con las habilidades que han aprendido durante la semana y cómo las aplicarán.

PAUSA [15]

14:45-15:45 (1 h)

- Elaboración de un plan de acción (continuación)
- Retroalimentación al grupo sobre los avances en su plan de acción

15:45-16:00 recapitulación, últimas preguntas y respuestas