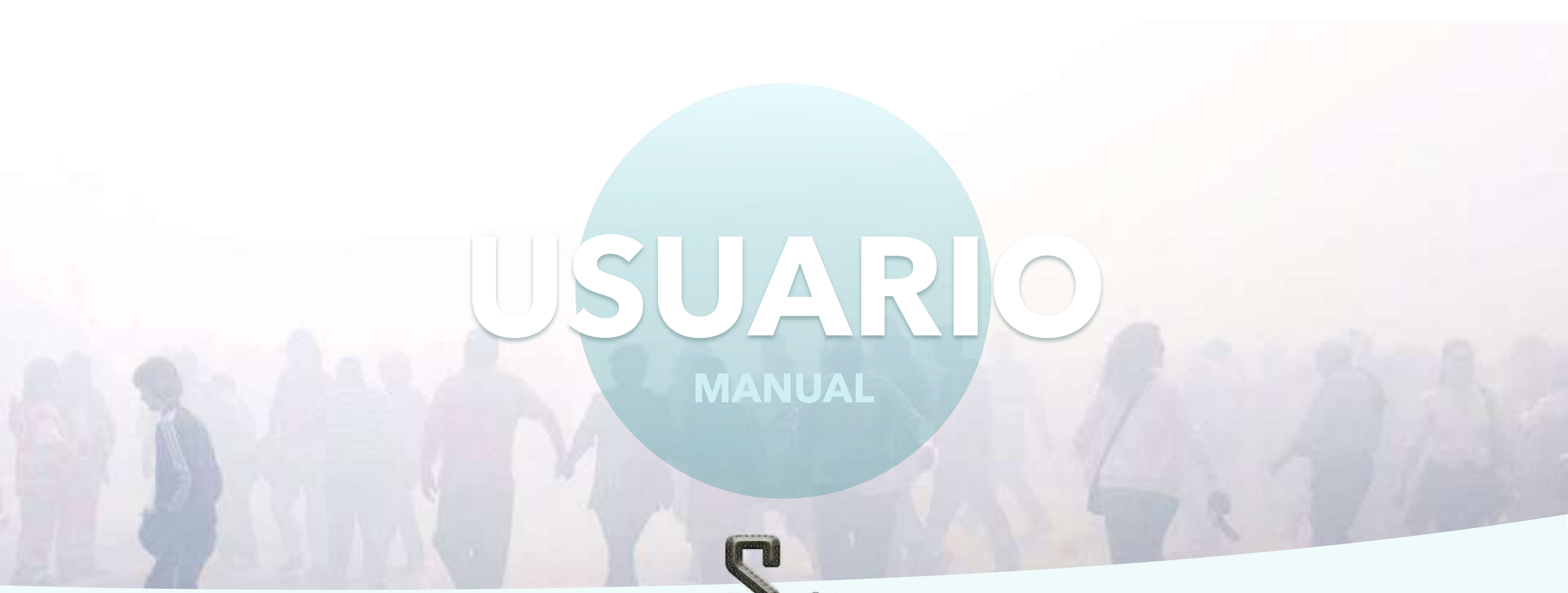


# USUARIO

## MANUAL

Safe

El presente documento establece la normativa a seguir por todo el personal que tiene acceso a los datos de carácter personal y a los sistemas de información de la organización. Siendo de obligado cumplimiento.

usuario
MANUAL

# Art. 32.4 Reglamento UE 2016/679 (RGPD)

"Todo responsable o encargado del tratamiento tomará las medidas oportunas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo las instrucciones del responsable."

Safe

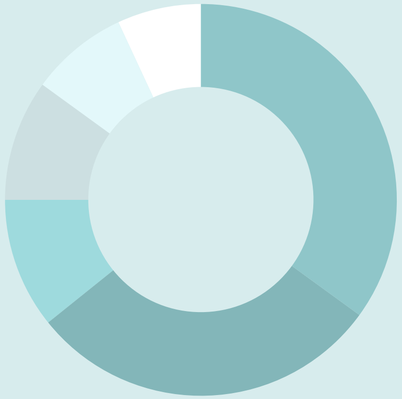
# conceptos

## DATOS PERSONALES

Toda información sobre una persona física identificada o identificable. Es decir, cuya identidad pueda determinarse, directa o indirectamente mediante un identificador, como por ejemplo un nombre, nº de identificación, datos de localización… etc.

## TRATAMIENTOS

Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o moificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.



Safe

## RESPONSABLE DEL TRATAMIENTO

La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento.

## ENCARGADO DE TRATAMIENTO

La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta de un responsable del tratamiento.

## FICHERO

Todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

## CONSENTIMIENTO

Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conicernen.

## INTERESADO

Persona titular de los datos, Es la persona cuyos datos de tratan, es decir: el cliente, paciente, ciudadano, proveedor, contacto, empleado… etc.

# conceptos

Safe

# responsable
## DE SEGURIDAD

**Tu organización dispone de una persona que se encarga de coordinar todo lo referente a protección de datos personales**

Esta persona se denomina "Responsable de Seguridad en materia de protección de datos personales". Es importante que conozcas quíen es pues es posible que necesites hacerle consultas.

Safe

# Tus obligaciones

## NORMAS GENERALES

Tienes algunas obligaciones importantes por tener acceso a datos de carácter personal.

Safe

1. Debes guardar el secreto respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la organización.

2. Almacena todos los soportes físicos y/o documentos que contengan información con datos de carácter personal en un lugar seguro, cuando estos no sen usados, particularmente fuera de la jornada laboral.

3. Queda prohibido el traslado de cualquier soporte, listado o documento con datos de carácter personal en los que se almacene información titularidad de la organización fuera de los locales de la misma sin autorización previa del Responsable de Seguridad.

4. Unicamente las personas autorizadas pueden introducir, modificar o anular los datos contenidos en los ficheros o documentos. En el caso de que requieras, para el desarrollo de tu trabajo, acceder a ficheros o documentos a cuyo acceso no estés autorizado, deberás ponerlo en conocimiento del responsable de seguridad.

5. Debes comunicar al responsable de seguridad, de forma inmediata, cualquier incidencia de seguridad de la que tengas conocimiento. Visita el apartado “violaciones de seguridad” para conocer qué se considera una violación de seguridad.

6. El deber de secreto se aplica también a tus contraseñas. Tienes obligación de poner en conocimiento del responsable de seguridad cualquier hecho que pueda haber comprometido el secreto. Las contraseñas de acceso son personales e intransferibles. Nunca utilices la misma contraseña en varios servicios ni las almacenes de forma que pueda ser accesible por un tercero.

7. Cierra y bloquea todas las sesiones al término de tu jornada laboral o si te ausentas tempralmente de tu puesto de trabajo, a fin de evitar accesos no autorizados.

8. Está prohibido copiar la información contenida en los ficheros en los que se almacenen datos de carácter personal a cualquier tipo de soporte sin autorización expresa.

9. Cuando envíes un documento a una impresora, ya sea propia o compartida, debes asegurarte de que no quede ningún documento en la bandeja de salida, que contenga datos de carácter personal. Debes retirar los documentos conforme vayan saliendo, con el fin de evitar que mientras se imprimen puedan ser leídos por personas no autorizadas.

10. Queda prohibido el envío de información de categorías especiales* sin autorización previa.

11. Queda prohibido, salvo autorización, la instalación de cualquier tipo de programa informático o el uso de dispositivos extraíbles.

12. Queda completamente prohibido el uso del correo electrónico corporativo para fines no relacionados con las funciones laborales encomendadas. El empleo del nombre o apellidos de los trabajadores o usuarios junto al dominio de la organización en las direcciones de correo no significa la asignación de la organización de un correo personal, esto se realiza únicamente por motivos organizativos internos de asignación de tareas y puesto de trabajo.

13 Es obligatorio que solicites autorización previa para en envío masivo de comunicaciones comerciales. En envío de comuniaciones a varios destinatarios se debe realizar siempre con copia oculta.

14 Almacena todos los soportes físicos y/o documentos que contengan información con datos de carácter personal en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.

15 Queda completamente prohibido el uso de Internet para tareas que no estén relacionadas directamente con las funciones asignadas al usuario. El organización regulará las modalidades de acceso y las restricciones o limitaciones del mismo.

16 Queda prohibido introducir contenidos en la red corporativa y/o dispositivos que no guarden relación con actividad y objetivos de la entidad.

17 Queda prohibido el uso de la red corporativa, sistemas informáticos o cualquier otro medio para vulnerar el derecho de terceros, los propios de la organización, o bien para la realización de acciones que puedan ser consideradas ilícitas.

18 En su caso, debes mantener debidamente custodiadas las llaves de acceso a las dependencias de la organización, a sus despachos y a los armarios, archivadores u otros elemantos que contengan ficheros con datos de carácter personal, debiendo poner en conocimiento del responsable de seguridad cualquier hecho que pueda haber comprometido su custodia.

*** Son considerados datos de categorías especiales:** origen étnico o racial, opniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos, datos de salud, datos de vida sexual u orientación sexual.

# Tus obligaciones

## NORMAS GENERALES

Safe

# protocolos

Conjunto de pautas establecidas por la organización para el tratamiento de datos de carácter personal.

Safe

## Obtención de datos

- Cualquier persona que facilite sus datos a la organización debe ser informada, previamente a la recogida de datos, de ciertos aspectos.
- En algunos casos el interesado, además, deberá haber otrogado también su consentimiento.
- La organización te proporcionará información sobre los métodos diseñados para poder realizar estos protocolos.

## Solicitudes de información

- Solo es posible facilitar datos de carácter personal al propio interesado o a su representante legal previa acreditación.

## Menores de edad

- En el ámbito de la protección de datos personales se consideran menores de edad a los menores de 14 años.
- Los menores de edad no pueden otorgar el consentimiento para el tratamiento de sus datos personales o solicitar el ejercicio de sus derechos.

Safe

## Destrucción de documentos

- Para poder destruir documentos debes estar autorizado. Si estás autorizado debes utilizar el método apropiado que ha sido diseñado por la organización.

## Uso de dispositivos

- La organización proporciona a los usuarios los equipos en buen estado, el usuario al recibirlos se compromete a cuidar de los dispositivos y hacer uso de ellos para los fines establecidos.
- Los dispositivos deben manipularse con el mayor cuidado, evitando golpes, rayones, presiones o temperaturas excesivas y ambientes muy contaminados. Se deben mantener los líquidos y otras sustancias nocivas alejadas de los dispositivos.
- Queda prohibida la apertura de dispositivos y la manipulación de sus componentes internos y sellos de garantía.
- Es obligación del usuario del dispositivo mantener actualizado el sistema operativo y el software, especialmente en lo relativo a fallos de seguridad.
- En caso de pérdida o daño por descuido o negligencia en el cumplimiento de este punto, su compensación económica podrá ser exigida al usuario.
- Queda prohibido el uso de dispositivos personales para fines corporativos sin autorización expresa.

Safe

## Uso del correo electrónico

- Debes prestar atención y ser proactivo en la detección de correos fraudulentos por ejemplo: cuando el cuerpo del mensaje presente cambios de aspecto, contenga una llamada a la acción urgente, o invite o solicite realizar una acción no habitual.
- Queda prohibida la apertura de emails sin, previamente, haber identificado al remitente. Si el remitente no es un contacto conocido se deberá prestar espacial atención ya que se puede tratar de un correo malicioso.
- Queda prohibido responder correos spam.
- Se prohibe el renvío de correos corporativos a cuentas personales.
- Se prohibe el acceso al correo electrónico corporativo desde conexiones públicas.

## Mesas limpias

- Los usuarios tienen la obligación de guardar la documentación de trabajo al ausentarse del puesto de trabajo y al terminar la jornada laboral. Queda prohibido dejar documentos con datos de carácter personal a la vista de personas no autorizadas.

## Dudas

- Ante cualquier duda sobre cualquier protocolo consulta con el responsable de seguridad.

Safe

# derechos

Aquellas personas que facilitan sus datos a la organización tienen algunos derechos que debes conocer.

Safe

# MUY IMPORTANTE

Negarse a actuar a petición del interesado con el fin de ejercer sus derechos supone una infracción que puede ser sancionada con multas administrativas de 20 millones de euros o el 4% del volumen de negocio total anual.

# acceso

A obtener, sin dilación indebida, del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y en tal caso, derecho de acceso a sus datos personales.

# limitación del tratamiento

El interesado tiene derecho a decidir para qué quiere que se utilicen sus datos.

# portabilidad

Tiene derecho a recibir los datos personales que le incumban, que haya facilitado, en un formato estructurado, de uso común y lectura mecánica y a transmitirlos a otro responsable.

# rectificación

El interesado tiene derecho a la rectificación de los datos inexactos que le conciernen.

# supresión

Tiene derecho a solicitar la supresión de los datos personales que le conciernen.

Safe

## ¿Qué debes hacer si te solicitan el ejercicio de un derecho?

1. Verificar la identidad del interesado mediante dni o documento equivalente. Obtener sus datos de contacto y averiguar exactamente qué tipo de derecho quiere solicitar.

2. Comunicar estos datos al responsable del tratamiento a la mayor brevedad.


# violación
## DE SEGURIDAD

Toda acción que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Safe

# ¿Qué se considera una violación de seguridad?

1. Acceso indiscriminado a datos personales.
2. Acceso a información confidencial.
3. Acceso no autorizado a los sistemas informáticos.
4. Pérdida de información.
5. Modificaciones y accesos no autorizados a datos.
6. Incumplimiento del protocolo de asignación, distribución y almacenamiento de contraseñas.
7. Borrado de datos no autorizado.
8. Traslado no autorizado de datos.
9. Transmisión ilícita de datos a un destinatario.
10. Vulneración del secreto profesional.
11. Disponer de un encargado de tratamiento sin la firma de un contrato.
12. Publicación de imágenes de personas identificables sin la autorización del interesado.
13. Envío de correos masivos sin ocultar los datos de los destinatarios (copia oculta).
14. Realizar transferencias internacionales de datos sin las garantías adecuadas de protección de datos.
15. Modificación de datos malintencionada.
16. Falsificación de datos.
17. Desinstalación de aplicaciones informáticas sin autorización.
18. Recuperación ineficaz de copias de seguridad.
19. Extravío u olvido de soportes.
20. Robo o sustracción de información.
21. No utilizar los métodos apropiados para la destrucción de papel o dispositivos.
22. Incendio, inundación u otras causas ajenas a la empresa.

Safe

## ¿Qué debes hacer si detectas una violación de seguridad?

Es muy importante que lo comuniques sin ninguna dilación al responsable de seguridad y que le facilites toda la información para que él pueda rellenar el documento habilitado a tal efecto.

Safe

www.safe-lopd.com

673 248 261

safe@safe-lopd.com