Confidencialidad y privacidad en la implementación del protocolo contra el acoso sexual y por razón de sexo en el ámbito del Trabajo

Semana Iberoamericana de la Buena Gestión en la Seguridad Social Madrid, 22 a 26 de mayo de 2023 Secretaría General de la Organización Iberoamericana de Seguridad Social (OISS)

Luis López Loma

El protocolo para la prevención y actuación frente al acoso sexual y el acoso por razón de sexo responde a la necesidad de prevenir, sensibilizar y, en su caso, atajar con todas las garantías estas formas de violencia y discriminación en el ámbito laboral, así como de cumplir con la legalidad vigente.

En España, este protocolo da cumplimiento a cuanto exigen los artículos 46.2 y 48 de la Ley orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres, el RD 901/2020 de 13 de octubre, por el que se regulan los planes de igualdad y su registro y se modifica el Real Decreto 713/2010, de 28 de mayo, sobre registro y depósito de convenios y acuerdos colectivos de trabajo y el artículo 14 de la Ley 31/1995, de 8 de noviembre, de prevención de riesgos laborales.

Una de las garantas que debe observarse para el desarrollo y aplicación del protocolo, entre otras, será la de respetar la confidencialidad. Es decir, será necesario proceder con la discreción necesaria para **proteger la intimidad y dignidad de las personas afectadas**. Las personas que intervengan en el procedimiento tienen la obligación de guardar una estricta **confidencialidad** y sigilo en todo momento.

REAL ACADEMIA ESPAÑOLA

confidencial

De *confidencia*.

1. adj. Que se hace o se dice en la confianza de que se mantendrá la reserva de lo hecho o lo dicho.
Información confidencial.

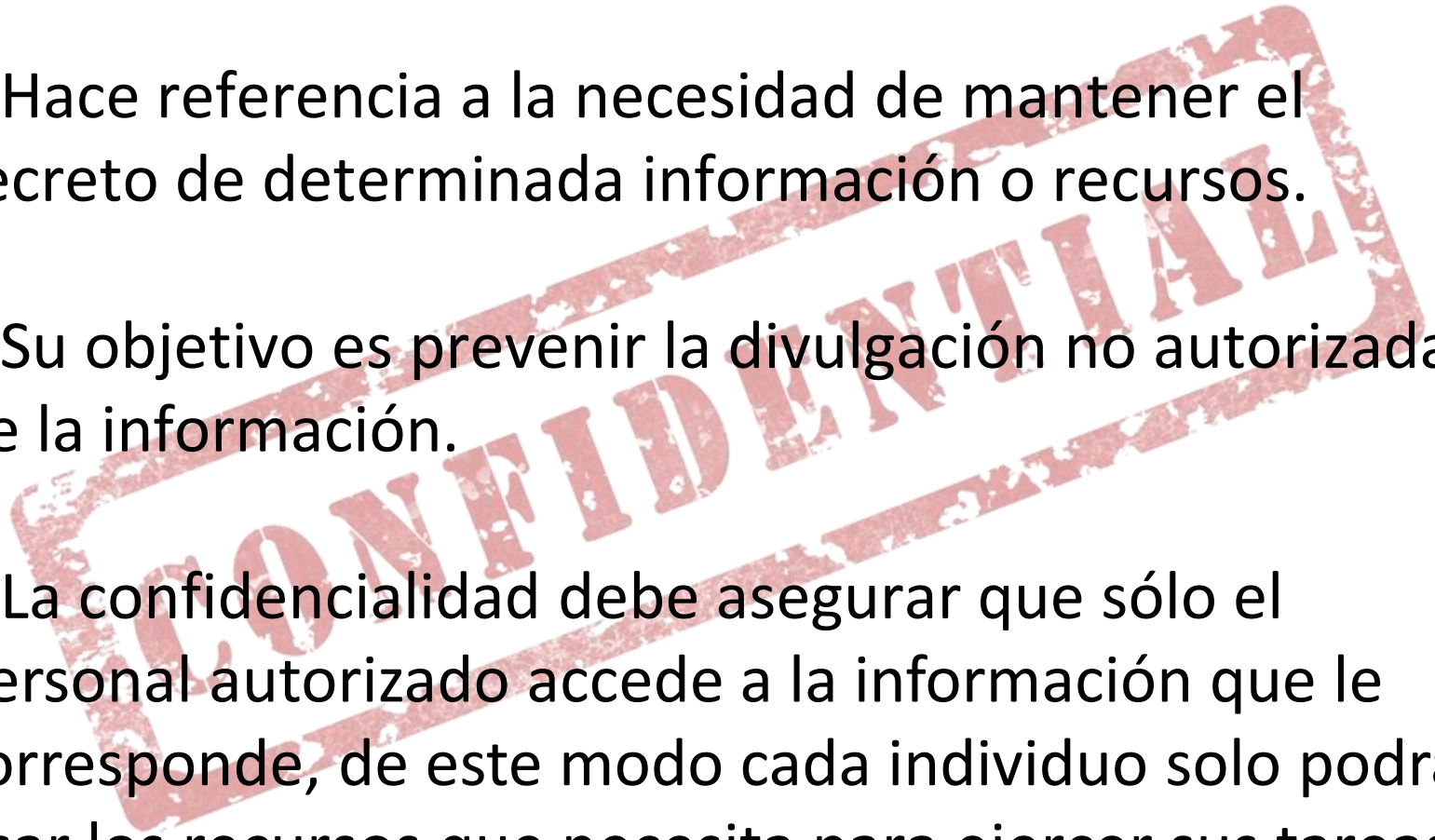

Confidencialidad
Seguridad
de la información
Integridad
Disponibilidad

Confidencialidad:

* Hace referencia a la necesidad de mantener el secreto de determinada información o recursos.

* Su objetivo es prevenir la divulgación no autorizada de la información.

* La confidencialidad debe asegurar que sólo el personal autorizado accede a la información que le corresponde, de este modo cada individuo solo podrá usar los recursos que necesita para ejercer sus tareas.



Cualquier tratamiento de dato de carácter personal, deberá cumplir con lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, o más conocido por sus siglas RGPD) y por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES Ley n.º 8968

ARTÍCULO 10.- Seguridad de los datos El responsable de la base de datos deberá adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a esta ley. Dichas medidas deberán incluir, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual, para garantizar la protección de la información almacenada.

No se registrarán datos personales en bases de datos que no reúnan las condiciones que garanticen plenamente su seguridad e integridad, así como la de los centros de tratamiento, equipos, sistemas y programas. Por vía de reglamento se establecerán los requisitos y las condiciones que deban reunir las bases de datos automatizadas y manuales, y de las personas que intervengan en el acopio, almacenamiento y uso de los datos.

ARTÍCULO 11.- Deber de confidencialidad La persona responsable y quienes intervengan en cualquier fase del tratamiento de datos personales están obligadas al secreto profesional o funcional, aun después de finalizada su relación con la base de datos. La persona obligada podrá ser relevado del deber de secreto por decisión judicial en lo estrictamente necesario y dentro de la causa que conoce.

PROTECCION DE LOS DATOS PERSONALES
Ley 25.326
Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales.

ARTICULO 9° — (Seguridad de los datos).
1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.
2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

ARTICULO 10. — (Deber de confidencialidad).
1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos.
2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

Ley N.° 29733
Ley de Protección de Datos Personales

Artículo 9. Principio de seguridad El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.

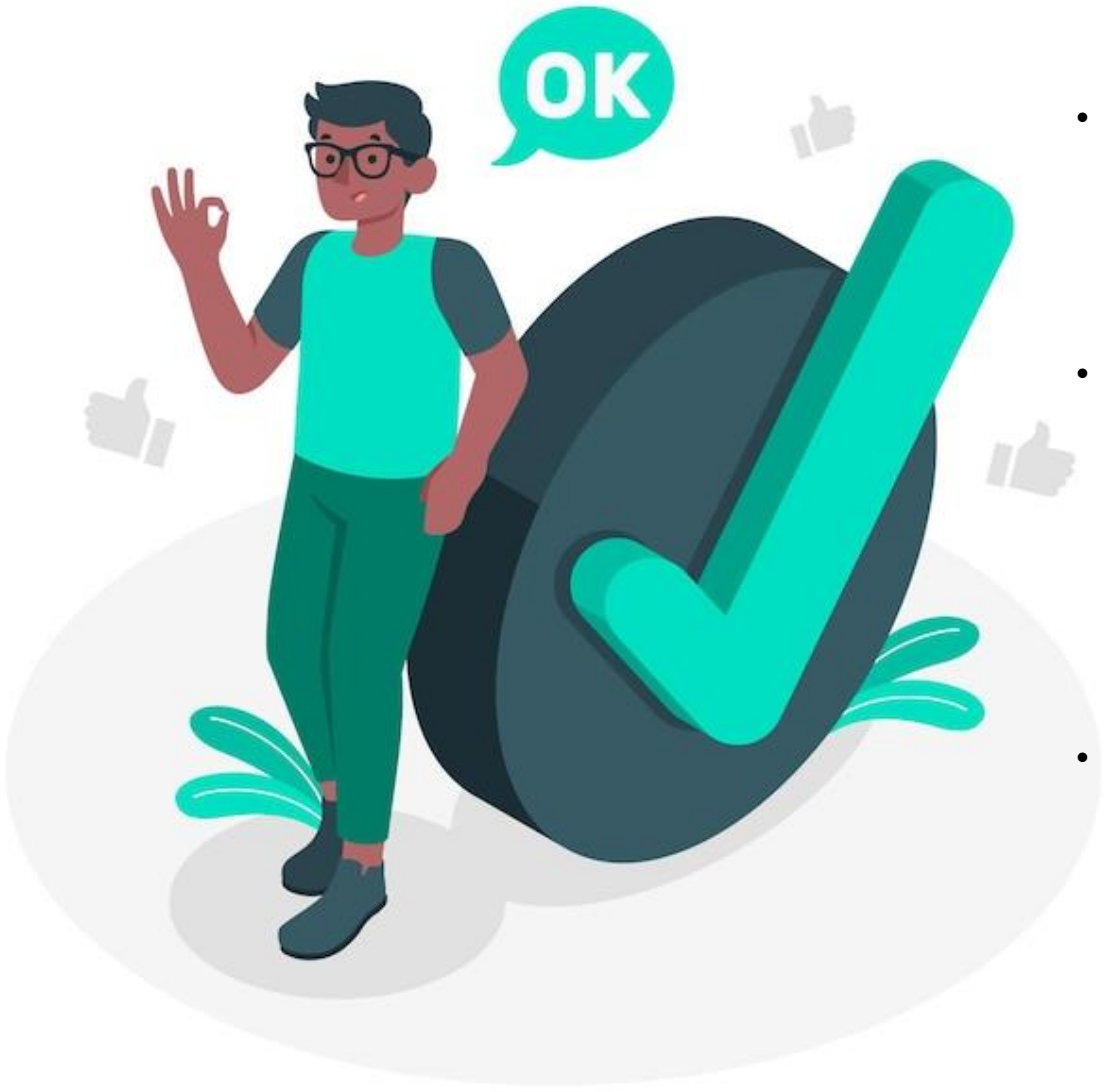
A fin de mantener la seguridad y evitar que el tratamiento de datos personales infrinja lo dispuesto en las normas relativas a la protección de datos, cada organización debe evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos.

Identificación de Riesgos

-¿Qué tecnologías se utiliza para el funcioamiento del canal de denuncias?
- ¿Mantenemos los sistemas informáticos al día?
- Sistemas de protección de los ordenadores. ¿Dispones de antivirus, cortafuegos o cifrado de discos y equipos?
- ¿Estamos formado internamente en conocer los riesgos del uso de la tecnología?
- ¿Tienes alguna política de gestión de contraseñas?
- ¿Qué se hace con la información, soportes, y sistemas que no vas a utilizar?
- ¿Se realizan copias de seguridad de equipos y correo? ¿Cada cuanto?

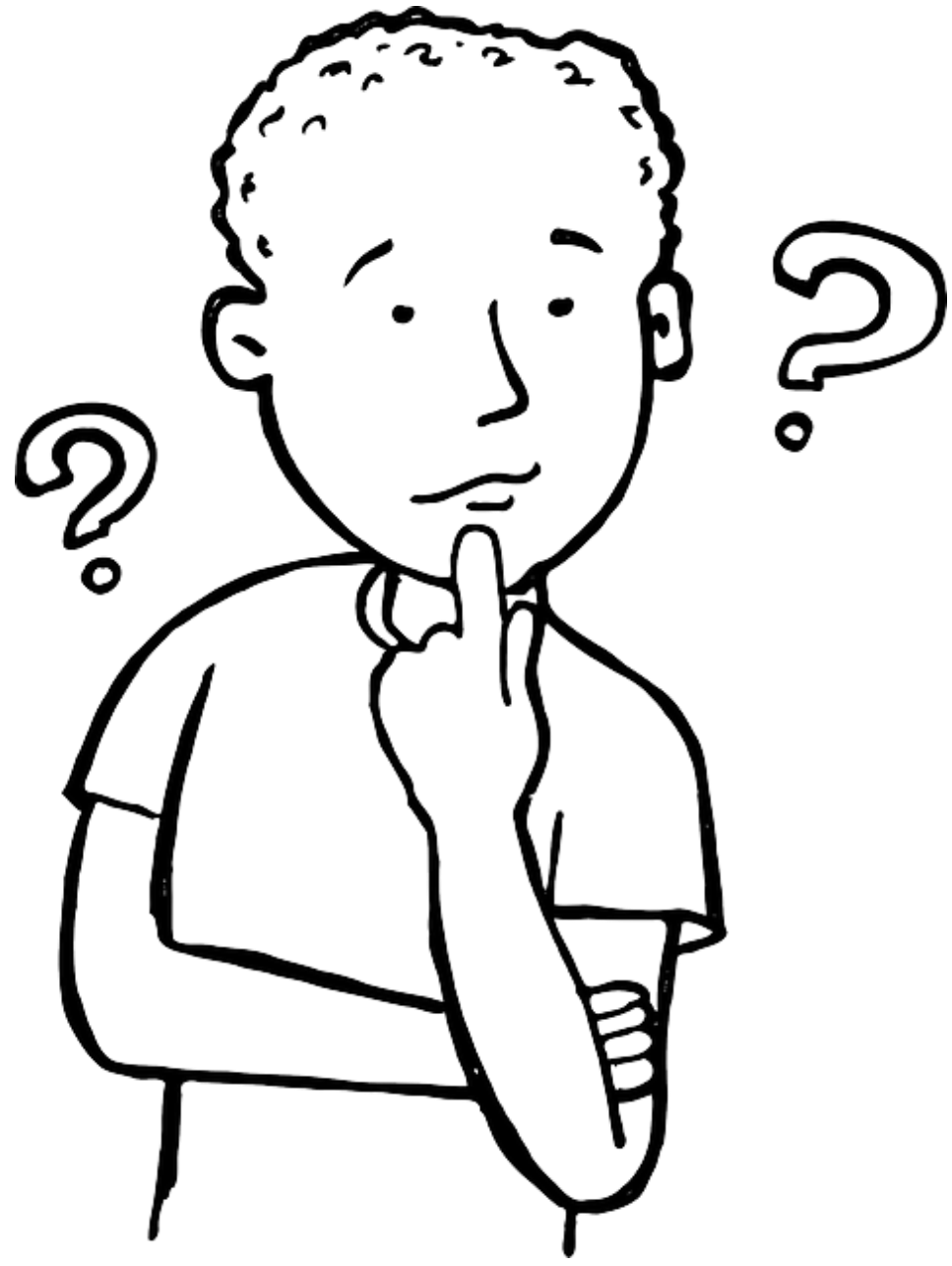
Establecer como canal de denuncia un correo electrónico general de la organización, puesto que vulneraría los principios analizados anteriormente, ya que:

- Si se trata de un buzón corporativo destinado a recibir, por ejemplo, las consultas planteadas por la web, a ser el canal de comunicación con los proveedores, etc. podría darse una pérdida o alteración accidental al eliminar el correo electrónico que manifieste una situación a investigar
- Si se trata de un buzón con acceso por parte de más de una persona, se produciría un acceso no autorizado.



Para garantizar la confidencialidad se pueden implementar principalmente las siguientes medidas técnicas:

- Sistemas de autenticación de usuarios: lo que permite identificar de forma unitaria al usuario que accede la información.
- Gestión de privilegios: lo que permite que los usuarios que acceden al sistema puedan operar sólo con la información para la que se les ha autorizado y sólo en la forma que se les autorice, por ejemplo, gestionando permisos de lectura o escritura en función del usuario.
- Sistemas de cifrado y encriptación: transforman la información de inteligible a no legible para que resulte incomprensible a aquellos usuarios que no disponen de los permisos para acceder a ella. Sin embargo, en estos sistemas existe un dato sensible que hay que proteger: la clave de encriptación.



IDENTIFICACIÓN Y AUTENTICACIÓN	SOLO FICHEROS AUTOMATIZADOS Identificación y autenticación personalizada. Procedimiento de asignación y distribución de contraseñas. Almacenamiento ininteligible de las contraseñas. Periodicidad del cambio de contraseñas (<1 año).	SOLO FICHEROS AUTOMATIZADOS Limite de intentos reiterados de acceso no autorizado.	
GESTIÓN DE SOPORTES	Inventario de soportes. Identificación del tipo de información que contienen, o sistema de etiquetado. Acceso restringido al lugar de almacenamiento. Autorización de las salidas de soportes (incluidas a través de e-mail) Medidas para el transporte y el desecho de soportes.	SOLO FICHEROS AUTOMATIZADOS Registro de entrada y salida de soportes: documento o soporte, fecha, emisor/destinatario, número, tipo de información, forma de envío, responsable autorizado para recepción/entrega.	SOLO FICHEROS AUTOMATIZADOS Sistema de etiquetado confidencial. Cifrado de datos en la distribución de soportes. Cifrado de información en dispositivos portátiles fuera de las instalaciones (evitar el uso de dispositivos que no permitan cifrado, o adoptar medidas alternativas).
COPIAS DE RESPALDO	SOLO FICHEROS AUTOMATIZADOS Copia de respaldo semanal. Procedimientos de generación de copias de respaldo y recuperación de datos. Verificación semestral de los procedimientos. Reconstrucción de los datos a partir de la última copia. Grabación manual en su caso, si existe documentación que lo permita. Pruebas con datos reales. Copia de seguridad y aplicación del nivel de seguridad correspondiente.		SOLO FICHEROS AUTOMATIZADOS Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.
CRITERIOS DE ARCHIVO	SOLO FICHEROS NO AUTOMATIZADOS El archivo de los documentos debe realizarse según criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO)		

RESPONSABLE DE SEGURIDAD		El responsable del fichero tiene que designar a uno o varios responsables de seguridad (no es una delegación de responsabilidad). El responsable de seguridad es el encargado de coordinar y controlar las medidas del documento.	
PERSONAL	Funciones y obligaciones de los diferentes usuarios o de los perfiles de usuarios claramente definidas y documentadas. Definición de las funciones de control y las autorizaciones delegadas por el responsable. Difusión entre el personal, de las normas que les afecten y de las consecuencias por su incumplimiento.		
INCIDENCIAS	Registro de incidencias: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras. Procedimiento de notificación y gestión de las incidencias.	SOLO FICHEROS AUTOMATIZADOS Anotar los procedimientos de recuperación, persona que lo ejecuta, datos restaurados, y en su caso, datos grabados manualmente. Autorización del responsable del fichero para la recuperación de datos.	
CONTROL DE ACCESO	Relación actualizada de usuarios y accesos autorizados. Control de accesos permitidos a cada usuario según las funciones asignadas. Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados. Concesión de permisos de acceso sólo por personal autorizado. Mismas condiciones para personal ajeno con acceso a los recursos de datos.	SOLO FICHEROS AUTOMATIZADOS Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información.	SOLO FICHEROS AUTOMATIZADOS Registro de accesos: usuario, hora, fichero, tipo de acceso, autorizado o denegado. Revisión mensual del registro por el responsable de seguridad. Conservación 2 años. No es necesario este registro si el responsable del fichero es una persona física y es el único usuario. SOLO FICHEROS NO AUTOMATIZADOS Control de accesos autorizados. Identificación accesos para documentos accesibles por múltiples usuarios.

ALMACENAMIENTO	SOLO FICHEROS NO AUTOMATIZADOS Dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura.		SOLO FICHEROS NO AUTOMATIZADOS Armarios, archivadores de documentos en áreas con acceso protegido mediante puertas con llave.
CUSTODIA SOPORTES	SOLO FICHEROS NO AUTOMATIZADOS Durante la revisión o tramitación de los documentos, la persona a cargo de los mismos debe ser diligente y custodiarla para evitar accesos no autorizados.		
COPIA O REPRODUCCIÓN			SOLO FICHEROS NO AUTOMATIZADOS Sólo puede realizarse por los usuarios autorizados. Destrucción de copias desechadas.
AUDITORIA		Al menos cada dos años, interna o externa. Debe realizarse ante modificaciones sustanciales en los sistemas de información con repercusiones en seguridad. Verificación y control de la adecuación de las medidas. Informe de detección de deficiencias y propuestas correctoras. Análisis del responsable de seguridad y conclusiones elevadas al responsable del fichero.	
TELECOMUNICACIONES			SOLO FICHEROS AUTOMATIZADOS Transmisión de datos a través de redes electrónicas cifradas.
TRASLADO DOCUMENTACIÓN			SOLO FICHEROS NO AUTOMATIZADOS Medidas que impidan el acceso o manipulación.


thank
you!!!