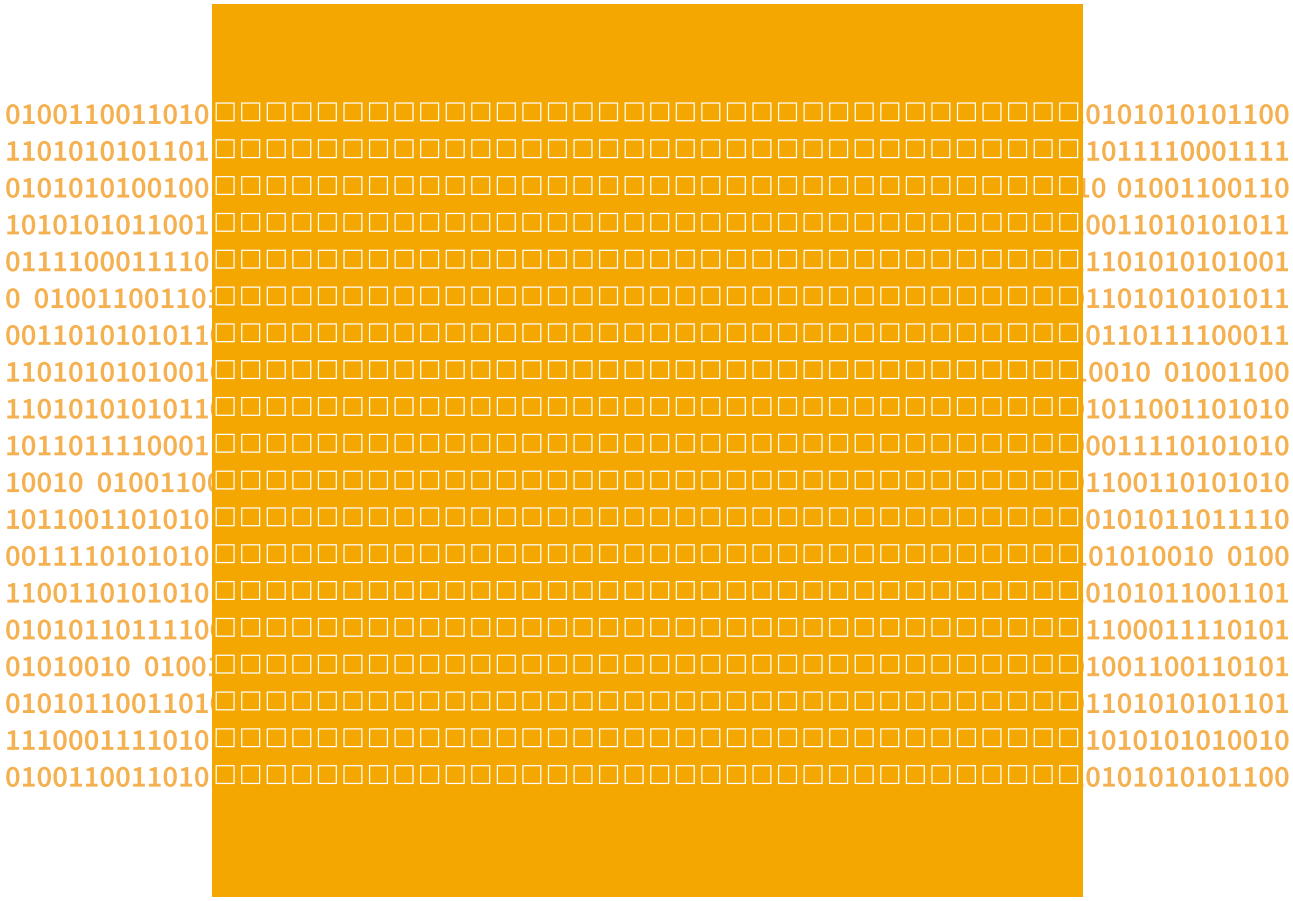
agencia española protección datos



AUTÓNOMOS Y PYMES

GUÍA DE CIFRADO

Publicada en
noviembre 2025

RESUMEN EJECUTIVO

El cifrado de la información es una herramienta cuyo uso debe ser fomentado en la tarea de proteger los datos personales y la seguridad de las comunicaciones en todos los ámbitos, también en el ámbito profesional.

Así lo expresa el Considerando 83 del Reglamento General de Protección de Datos, cuando afirma que "a fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado".

Esta guía va dirigida a profesionales autónomos y pequeñas y medianas empresas (PYMES), al objeto de proporcionarles un enfoque práctico que les facilite implementar medidas de cifrado seguras y adecuadas en distintos escenarios, como pueden ser: el envío de correos electrónicos, el almacenamiento en la nube y la protección de la información almacenada en dispositivos.

En la guía se analizan sucesos reales destacados de diversos sectores, donde pueden observarse las graves consecuencias de no aplicar las medidas de protección mínimas, que pueden derivar no solo en filtraciones de datos, fraudes o suplantación de identidad, sino también en graves perjuicios a la integridad física o psicológica de las personas, además de las consecuencias, administrativas y de otro orden, que deberán afrontar los responsables.

Asimismo, se subraya la importancia de adoptar medidas que garanticen la protección de datos, es decir, medidas de privacidad. Nos referimos, en particular, a la aplicación del principio de minimización de datos, que asegura que solo se trate la información estrictamente necesaria en cada fase del tratamiento y para su finalidad específica, y que permite reducir el impacto sobre los individuos cuando fallan las medidas de seguridad.

A lo largo del documento, se proporcionan herramientas y recursos para ayudar a los profesionales y a las PYMES a mejorar la seguridad de la información, minimizando los riesgos para los individuos y cumpliendo con la normativa de protección de datos vigente.

Claves: Privacidad, RGPD, internet, protección de datos, ciberseguridad, brecha, cifrado, contraseña, datos, riesgos, anonimización, autenticación, credenciales, datos personales, email, fraude, seudonimización, ataque, nube, correo, criptografía.

ÍNDICE

I. OBJETIVO Y DESTINATARIOS

El objetivo de esta guía es proporcionar a profesionales autónomos y a pequeñas y medianas empresas (pymes) las herramientas y conocimientos necesarios para implementar el cifrado de datos de manera efectiva en sus operaciones. El cifrado consiste en transformar la información en un formato ilegible para cualquiera que no disponga de la clave de descifrado. De esta forma, solo las personas autorizadas pueden acceder a los datos[1].

Esta guía está dirigida a quienes tratan datos personales, que en algunos casos pueden incluir datos sensibles, como datos personales de clientes o registros financieros, y deben garantizar la protección de los derechos y libertades de aquellos terceros, personas físicas identificadas o identificables, cuyos datos personales son objeto de tratamiento. Su objetivo es mitigar el impacto de brechas de datos personales, protegiendo la confidencialidad, integridad y disponibilidad de la información. Además, como efecto colateral deseable, contribuye a proteger el objeto de negocio frente a accesos no autorizados.

Los casos de uso analizados en esta guía, extraídos de brechas reales que se han comunicado y denunciado a la AEPD, reflejan situaciones en las que la falta de medidas de seguridad en el tratamiento de la información ha tenido consecuencias graves para las personas físicas. Las Secciones IV y V proporcionan soluciones basadas en el cifrado que, de haberse aplicado previamente, habrían mitigado o evitado los problemas descritos.

II. ¿QUÉ PUEDE PASAR SI NO SE CIFRA LA INFORMACIÓN?

En primer lugar, la entidad responsable del manejo de datos personales, propios o de terceros, debe ser consciente de qué tratamientos implican un riesgo para las personas físicas: aquellos que puedan tener un importante impacto sobre los derechos y libertades de las personas, pudiendo llegar en algunos casos a impactos a su integridad física. Hay que reflexionar sobre el impacto que pueden tener los tratamientos de datos personales que se realizan en el marco de cualquier actividad e incorporar las salvaguardas necesarias para minimizar o, incluso, eliminar los posibles riesgos.

El impacto de una brecha puede ser grave, aunque no afecte a categorías especiales de datos. Por ejemplo, una dirección o un teléfono no son categorías especiales de datos, pero cuando están vinculados a víctimas de violencia de género, su revelación a terceros puede tener un impacto fatal en la integridad física de las personas.

Si los tratamientos de datos no se realizan incorporando medidas de seguridad adecuadas, los datos personales pueden ser interceptados, robados o expuestos, lo que incrementa

[1] Ver las Orientaciones para la validación de sistemas criptográficos en la protección de datos y la herramienta asociada Valida-Cripto RGPD

el riesgo de accesos no autorizados, manipulaciones indebidas, suplantación de identidad, fraudes, ataques personales o virtuales y otros delitos.

Además, un manejo inadecuado de información sensible puede derivar en graves consecuencias para las personas afectadas, como discriminación, acoso, violencia o incluso poner en peligro su integridad física, además de daños reputacionales e incumplimientos legales. No debemos olvidar que la falta de salvaguardas organizativas, legales y técnicas adecuadas en el tratamiento de datos puede conllevar, además, responsabilidades civiles o penales, así como sanciones administrativas por vulnerar normativas de protección de datos.

A continuación, se presentan **ejemplos** de fallos en el tratamiento de información que han desencadenado graves consecuencias en diferentes ámbitos:

A. DISPOSITIVO PERDIDO: FILTRACIÓN DE DATOS CONFIDENCIALES DE MENORES EN LA DARK WEB

Un psicólogo que da servicio a un centro de educación primaria extravía un portátil que contenía los expedientes escolares de alumnos presentes y pasados. Entre los datos se encontraban nombres, fotografías, direcciones, teléfonos, correos, horarios, actividades extraescolares, rutas de autobús, etc, de menores. Posteriormente, se detecta que dicha información se difunde por la dark web en círculos de trata de menores. Dichos datos permiten localizar a los menores tanto a través de Internet como físicamente, exponiéndolos a acoso por parte de pedófilos o incluso secuestros.

¿Tendría que haberse cifrado el disco duro?

Solo en marzo de este año, la AEPD recibió casi 170 notificaciones de brechas de datos personales que afectaban a la confidencialidad de la información y un 50% de ellas se debieron a la exfiltración de datos, **pérdida de dispositivos** o comunicaciones de datos personales que no estaban adecuadamente cifrados.

Los dispositivos que contienen datos con un alto impacto potencial y que se utilizan fuera de entornos seguros deben estar apropiadamente cifrados. Este caso en particular es significativo por el número de veces que se ha producido.

Se debe tener en cuenta también que el cifrado de la información, que es una medida de seguridad esencial contemplada en el RGPD, no basta por sí solo. La mejor medida para proteger los datos de menores en los dispositivos portátiles es minimizar la cantidad de datos que se guardan en ellos, conservando -exclusivamente- aquellos que sean indispensables para cumplir con la finalidad para la cual fueron recogidos.

DISPOSITIVO PERDIDO

¿En qué aspectos hay que involucrarse?

En este caso se ha producido una grave brecha de la confidencialidad de datos especialmente sensibles, como son datos relacionados con menores. Independientemente de haber aplicado medidas de cifrado, ante tal suceso se debe notificar inmediatamente el incidente al responsable de protección de datos del centro y a las autoridades competentes, ya que puede implicar un alto riesgo para los derechos de los afectados. Asimismo, debe valorarse si el responsable debe comunicar[2] a las personas interesadas de forma inmediata (en este caso, aquellos que ejercen la patria potestad o tutela de los menores) la información necesaria para que sean conscientes de los riesgos que ha provocado esta situación y que adopten las medidas adecuadas para poder minimizarlos.

¿Deberían haberse protegido los archivos de forma diferente?

Sí, además del cifrado del disco duro se podrían haber protegido los archivos cifrándolos individualmente antes de almacenarlos en el portátil. Eso habría minimizado el riesgo de exposición en caso de pérdida o robo del dispositivo, sin perjuicio de que se hayan aplicado otras medidas de privacidad consistentes en: evaluar la estricta necesidad de sacar dicha información del centro, aplicar criterios de minimización y seudonimización en la recogida y almacenamiento de datos, eliminar información sobre menores cuando ya no sea necesaria, establecer contraseñas para restringir el acceso y seguir protocolos de seguridad del centro educativo.

¿Cómo se podría haber evitado este caso?

La pérdida de un portátil con información confidencial de alumnos supone un riesgo significativo, ya que terceros podrían acceder a datos personales, fotografías, direcciones o itinerarios.

Si el **disco duro del ordenador estuviera cifrado**, incluso si el dispositivo cayera en manos equivocadas, conseguiría dificultar o impedir el acceso a la información almacenada, lo que permitiría tanto al centro como a las partes interesadas tomar las medidas adecuadas de protección. Implementar medidas de acceso restringido, como la autenticación en dos pasos y el borrado remoto del dispositivo, añadiría una capa adicional de protección ante este tipo de incidentes.

[2] La comunicación de brechas de datos personales se encuentra explicada en detalle en la Guía para la notificación de brechas de datos y la infografía Proteger a las personas en el mundo digital de la AEPD.

B. PUBLICACIÓN NO INTENCIONADA: EXPOSICIÓN DE DATOS SENSIBLES DE PLANIFICACIÓN FAMILIAR EN INTERNET

Un médico de una clínica de planificación familiar tiene todos los datos de sus intervenciones almacenadas en una tabla que no está cifrada. Al instalarse en su ordenador una aplicación de compartición de archivos, por error, comparte públicamente dicha tabla. Los datos de muchas mujeres que realizaron la interrupción voluntaria del embarazo han quedado libremente expuestos en Internet con consecuencias familiares y sociales. Incluso, algunas de esas mujeres son residentes de países en los que les tienen prohibido ejercer sus derechos y que pueden afrontar consecuencias peores que las penales.

¿Hay responsabilidad?

Sí, el médico y la clínica tienen responsabilidad legal, ya que han incumplido con las normativas de protección de datos al no garantizar la seguridad de información sensible custodiada por ellos. Este supuesto puede calificarse de brecha de confidencialidad de datos personales, que debe ser notificada a la AEPD e inmediatamente comunicada a los interesados, asumiendo la responsabilidad, e incluyendo asesoramiento para minimizar el impacto que sobre ellos pudiera tener esta brecha[3]. Adicionalmente, también pueden tener responsabilidad deontológica, por no haber protegido adecuadamente las obligaciones de secreto profesional que pueden resultar aplicables.

¿Estaban los datos cifrados?

No, en este caso los datos no estaban cifrados, lo que permitió que fueran fácilmente accesibles por terceros cuando se compartieron accidentalmente. Si hubieran estado correctamente cifrados, aunque se hubieran expuesto, el acceso a la información hubiera sido muchísimo más complejo y hubiera requerido mucho tiempo y recursos. Además, al no estar disponibles para un público general, hubiera resultado más fácil la retirada del contenido en línea. Esto resalta la importancia del cifrado como medida esencial en la protección de datos sensibles. En las **Secciones IV y V** se presentan algunas herramientas para poder aplicar técnicas de cifrado de la información.

Además del cifrado, otras prácticas que pudieron haber mitigado el impacto de esta filtración serían la seudonimización y la minimización de los datos, que consisten, la primera en sustituir los nombres completos de los pacientes por códigos solamente descifrables por el responsable del tratamiento, y la segunda en almacenar la información estrictamente necesaria, durante el tiempo imprescindible, y evitar incluir datos personales que puedan identificar directamente a las pacientes. Esto habría reducido significativamente el riesgo de acceso no autorizado a la información en caso de una brecha de seguridad.

[3] La AEPD publica una guía dirigida a los profesionales del sector sanitario | AEPD

PUBLICACIÓN NO INTENCIONADA

¿Cómo se podría haber evitado este caso?

El envío accidental del registro de tratamientos de pacientes representa una grave vulneración de la confidencialidad. Si los ficheros de los pacientes estuvieran **cifrados** antes de ser publicados o enviados, solo el destinatario autorizado con la clave para descifrarlo podría acceder a su contenido. Además, en el ámbito profesional, el uso de **correos electrónicos cifrados y plataformas seguras** para compartir archivos también ayudaría a reducir aún más estos riesgos, garantizando una mayor protección de la información. También debe considerarse que, en el caso de tener que distribuirse la clave de descifrado que es la que permite acceder a la información en formato legible, tal distribución debe realizarse por un medio distinto al utilizado para enviar los ficheros, por ejemplo, mediante una llamada telefónica, un mensaje SMS seguro o el uso de un gestor de contraseñas compartido, asegurando que, en caso de un envío erróneo, los datos permanezcan inaccesibles. Implementar controles de acceso estrictos, auditorías de seguridad periódicas y mecanismos de doble verificación en el envío de información confidencial reforzaría aún más la protección de los datos médicos.

C. ENVÍO ERRÓNEO DE CORREO ELECTRÓNICO: REVELACIÓN DE INFORMACIÓN CONFIDENCIAL A LA PERSONA INCORRECTA

Un abogado envía por correo electrónico un documento legal cifrado a su cliente. En el mismo mensaje indica que la contraseña para descifrarlo corresponde al DNI de este. Por error, el abogado envía el correo a la expareja de su cliente, quien tiene una orden de alejamiento por violencia de género. Dado que conoce el DNI de su expareja, puede acceder a la información confidencial del mensaje. Además, el abogado incluyó detalles innecesarios en el asunto del correo, lo que agrava la exposición de la información.

¿Es seguro enviar documentos cifrados por correo electrónico?

La seguridad de la información cifrada depende, entre otros aspectos, de cómo se maneje la clave de descifrado. En este caso, incluir la contraseña en el mismo mensaje (p.ej. un correo electrónico) anula la seguridad del cifrado, ya que de interceptarse el correo puede tenerse acceso a la clave de cifrado de los ficheros adjuntos. Incluir pistas o información que ayuden a averiguar la clave es una práctica que también anula la eficacia del cifrado. En estos casos, lo ideal es compartir la clave por un canal separado, que no sea evidente, ni que sea información fácil de inferir por un tercero (p.ej. a través de una llamada o un mensaje de texto alternativo, o usar claves evidentes como el teléfono o el DNI del destinatario). Enviar la clave por el mismo medio, por ejemplo, el

ENVÍO ERRÓNEO DE E-MAIL

correo, pero en dos mensajes separados no es una práctica totalmente efectiva, ya que, si el canal ha sido comprometido, el atacante tendrá acceso a tos los mensajes intercambiados por el mismo[4]. También es fundamental verificar siempre la dirección del destinatario antes de enviar información confidencial para evitar errores humanos que puedan comprometer la seguridad de los datos.

¿El contenido del asunto del correo puede agravar las consecuencias?

Sí. Si el asunto del correo contiene información innecesaria, sensible o que haga evidente el contenido del mensaje, podría aumentar el riesgo de exposición y agravar la responsabilidad del remitente y las consecuencias para el cliente. En este caso, revelar detalles sobre el cliente o el tipo de documento en el asunto podría facilitar el descifrado y, por ende, el acceso indebido a la información, constituyendo un posible incumplimiento de las obligaciones de la normativa de protección de datos, además de la obligación de mantener el secreto profesional recogido en el código deontológico de la Abogacía.

¿Cómo se podría haber evitado este caso?

El envío erróneo de un documento legal a un destinatario no autorizado supone una vulneración de la **confidencialidad**, especialmente en la situación mencionada. Aunque el documento esté cifrado, incluir la clave en el mismo correo elimina cualquier protección que el cifrado pudiera ofrecer, permitiendo el **acceso indebido** a datos sensibles.

Para evitar este tipo de errores, es fundamental emplear plataformas seguras de intercambio de documentos y utilizar métodos de autenticación más robustos. Además, la contraseña de acceso nunca debe enviarse en el mismo mensaje que el documento cifrado, sino a través de un **canal seguro y distinto**.

También es esencial redactar los asuntos de los correos electrónicos con neutralidad y prudencia para no revelar información innecesaria que pueda agravar la exposición de los datos.

[4] Por ejemplo, la DIRECTIVA (UE) 2015/2366 (PSD2) establece que, cuando sea necesaria una autenticación reforzada en su ámbito de aplicación, esta debe basarse en la utilización de dos o más elementos categorizados como conocimiento (algo que solo conoce el usuario), posesión (algo que solo posee el usuario) e inherencia (algo que es el usuario), los cuales deben ser independientes entre sí, es decir, de modo que la vulneración de uno no comprometa la fiabilidad de los demás, y concebida de manera que se proteja la confidencialidad de los datos de autenticación (art.4.30)

D. ACCESO NO AUTORIZADO A DATOS EN SISTEMA DE INFORMACIÓN POR ABUSO DE PRIVILEGIOS DE UN SERVICIO EXTERNO

Una gestoría lleva la administración de fincas y seguros de un gran número de propietarios. Tiene una copia de seguridad almacenada en servicios de terceros que no se encuentra cifrada. Dicha copia ha sido accesible debido a una negligencia, o una venta de datos fraudulenta, del personal de dicho servicio. Los datos permiten identificar, entre otras, a personas de edad avanzada, que viven solas, la dirección de estas y la evaluación de sus bienes incluyendo sus datos financieros. Todas ellas quedan expuestas a estafas o incluso a asaltos en sus propios hogares.

¿Son datos personales?

En los ocho casos expuestos en esta sección, los datos que manejan los distintos profesionales son datos personales, (Art. 4.1)[5]. En este caso, la información contiene el nombre, un número de identificación, datos bancarios y datos de localización que permiten que una persona sea identificable o identificada.

¿Es legal almacenar información de propietarios en la nube?

Los datos personales, una vez cifrados, continúan siendo datos personales. Los datos personales se pueden almacenar en servicios de terceros, por ejemplo, la nube. Sin embargo, el contratar un encargado no supone un desvío de la responsabilidad exigible por el RGPD a un tercero. El responsable debe seleccionar diligentemente un tercero que garantice, por contrato, el cumplimiento de la normativa de protección de datos, en particular, los requisitos del Art. 28 del RGPD en cuanto a la relación con un encargado y los niveles de calidad de servicio que garanticen la necesaria disponibilidad que exige el Art. 32 del RGPD, e incluso -en algunos casos- gestionar la resiliencia del tratamiento con medios propios u otros terceros. Además, el tercero debe almacenar los datos en servidores seguros, utilizando técnicas como acceso restringido a los ficheros y el cifrado de estos. En el caso de que el proveedor de la nube esté fuera del país, también se deben cumplir las condiciones para las transferencias internacionales de datos.

¿Cómo se podría haber evitado este caso?

Cuando se contrata un servicio en la nube, hay que asegurarse que el proveedor mantiene los datos almacenados cifrados. Además, hay que comprobar si recientemente han existido en dicho proveedor incidentes de seguridad o está sometido a legislaciones que le obligan a proporcionar datos a sus autoridades.

Implementar un **cifrado previo de los archivos** y utilizar plataformas con **cifrado de extremo a extremo** garantizaría que solo las partes autorizadas accedan a la información. También es recomendable utilizar autenticación en dos pasos para reforzar la seguridad del acceso y monitorear la actividad en la nube para detectar posibles intentos de intrusión o filtraciones de datos. Además, establecer políticas de acceso restringido y consultar periódicamente a especialistas sobre la seguridad real de dicho servicio contribuiría a una mejor protección de la información confidencial.

E. ENVÍO DE CORREO ELECTRÓNICO A MÚLTIPLES DESTINATARIOS POR ERROR, DIVULGANDO INFORMACIÓN CONFIDENCIAL

Un empleado de una agencia de viajes envía a la central un fichero con todos los contratos de viaje realizados para las próximas vacaciones. Por error, al escribir la dirección de correo se equivoca y la envía a una multiplicidad de personas. En dicho fichero se encuentran las direcciones postales de personas que se van de vacaciones y las fechas en las que sus casas estarán vacías. Esta filtración expone a los clientes a posibles robos, ya que terceros pueden aprovechar la información para planear asaltos en ausencia de los propietarios.

¿Podría haber pasado lo mismo si no se hubiera enviado la información?

Todo almacenamiento de datos está expuesto a la posibilidad de robo de información e intrusiones de acceso a la información, pero también al error humano que no necesariamente tiene una intención de dolo. Hay que asumir la realidad de que somos humanos y una situación de estrés nos puede conducir a cometer errores.

¿Qué medidas se pueden tomar para evitar un incidente así en el futuro?

Se debe establecer un protocolo para manejar información confidencial que incluya el uso de herramientas seguras para compartir datos, como plataformas cifradas, que, si bien no evitarían un envío erróneo, sí contribuirían a mitigar el riesgo de divulgación no autorizada. Además, reforzar la formación sobre privacidad y verificar cuidadosamente los destinatarios antes de enviar información, asegurando que se comparte solo lo indispensable.

¿Cómo se podría haber evitado este caso?

El envío accidental de un registro confidencial de viajeros supone un riesgo significativo, ya que terceros podrían acceder a datos como cuentas bancarias, itinerarios o números de pasaportes.

Para evitar este tipo de incidentes, es fundamental cifrar los documentos que contienen información sensible, limitando el acceso a las personas autorizadas. Además, utilizar **herramientas de cifrado** para proteger los archivos antes de su envío y evitar compartir documentos mediante medios inseguros minimizaría el riesgo de filtración de datos. Implementar medidas adicionales, como el uso de plataformas seguras de transferencia de archivos, la autenticación en dos pasos y controles estrictos sobre los destinatarios, la sensibilización de los trabajadores o la revisión de los procesos, reforzaría la seguridad y reduciría la posibilidad de errores humanos.

[5] 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).

F. ABUSO DE PRIVILEGIOS DE ACCESO: DIVULGACIÓN NO AUTORIZADA DE DATOS SENSIBLES CON FINES DISCRIMINATORIOS

Un laboratorio lleva a cabo estudios de ADN humano. Las muestras, los resultados, así como otra información personal adicional, son almacenados en una base de datos sin cifrar. En el contexto internacional surge una guerra étnica con dramáticas consecuencias. Alguien con permisos de administración y acceso a la base de datos, la filtra para que terceros seleccionen por ADN datos potenciales de personas asociadas al grupo rival. Aunque se identifica el origen de la información, esta ya aparece en grupos violentos de Telegram que promueven ataques contra las personas afectadas y, por extensión, contra sus familiares.

¿Cómo se debería haber protegido la base de datos para evitar este incidente?

Además del cifrado como medida básica y esencial, debería haberse implementado un control de acceso estricto y estrategias de privacidad que garantizaran la eliminación o seudonimización[6] de los identificadores y datos personales. Asimismo, la cancelación o anonimización de los datos debería haberse realizado tan pronto como dejaran de ser estrictamente necesarios. El manejo de datos genéticos requiere un nivel de seguridad aún mayor debido a su sensibilidad, el impacto en el entorno de la persona afectada y sus posibles implicaciones éticas. La publicación accidental de datos genéticos o de salud podría derivar en discriminación, delitos de odio, ataques, consecuencias psicológicas o incluso repercusiones legales.

¿Qué impacto tiene la filtración de estos datos en la seguridad de los afectados?

La exposición de información genética en un contexto de conflicto puede poner en peligro la vida de las personas afectadas y de sus familiares. La discriminación genética puede derivar en persecución, exclusión de servicios o violencia selectiva, como se ha visto en conflictos con componentes étnicos. Estos hechos subrayan la necesidad de tratar los datos con un nivel máximo de seguridad y confidencialidad. Además, los datos genéticos son **irremplazables** (a diferencia de una contraseña), por lo que una filtración tiene consecuencias permanentes para las personas afectadas.

¿Cómo se podría haber evitado este caso?

La publicación de información relativa al ADN se podría haberse evitado mediante la implementación de estrictas medidas de seguridad y privacidad en la gestión de los datos genéticos. En primer lugar, la base de datos debería haber estado cifrada tanto en reposo como en tránsito, asegurando que incluso si alguien accedía a ella, la información no pudiera ser fácilmente leída o utilizada. Además, se debería haber aplicado el principio de **mínimos privilegios**, limitando el acceso a los datos solo a quienes realmente lo necesiten y estableciendo **controles de acceso granulares**. La **auditoría y monitorización continua** de accesos a la base de datos habrían permitido detectar comportamientos sospechosos a tiempo. También sería fundamental la implementación de medidas de **trazabilidad** y de doble factor de autenticación (**2FA**) para la extracción de información sensible, evitando que una sola persona con permisos de administrador pudiera acceder y filtrar todos los datos sin supervisión.

G. INCIDENCIA TÉCNICA: EXPOSICIÓN PÚBLICA EN INTERNET DE HÁBITOS PERSONALES DE USUARIOS

Una app de corredores (móvil o pulsera) guarda en un servidor las rutas de los usuarios suscritos. Estas rutas solo están asociadas a un identificador numérico y a ciertos parámetros, como la hora de la carrera, el sexo o la edad, y son accesibles únicamente para cada corredor. Debido a un error en la configuración del servidor, la base de datos queda expuesta a Internet. Se pueden identificar rutas populares, ya que son seguidas por muchos corredores. Sin embargo, también se observan otras muy poco transitadas, algunas de ellas utilizadas únicamente por un solo corredor, en horarios solitarios y con información sobre su sexo.

¿Se consideran datos personales si solo hay identificadores numéricos y parámetros como sexo o edad?

Sí, aunque no se almacenen nombres, los identificadores únicos son datos personales si permiten identificar indirectamente a una persona, singularizándola, permitiendo realizar acciones específicamente dirigidas a ella combinándose con otros datos, como localizaciones, patrones de movimiento o características específicas.

¿Qué riesgos implica que estas rutas sean accesibles públicamente?

El principal riesgo es la seguridad física de los corredores, especialmente en rutas solitarias o poco transitadas. Un atacante podría identificar hábitos, horarios y recorridos de ciertas personas, aumentando el riesgo de acecho, acoso o agresiones. Con datos adicionales se podría determinar cuáles podrían ser objetivos más vulnerables, como menores. También hay un riesgo de suplantación de identidad si alguien cruza los datos con otra fuente de información. Para mitigar esto, la app debería implementar cifrado en la base de datos, restringir el acceso con autenticación robusta y anonimizar aún más los datos o introducir información de falsos recorridos de personas imaginarias para evitar la existencia de casos singulares. Además, existe la posibilidad de un impacto general a la seguridad, como revelar información sobre infraestructuras críticas, como instalaciones de seguridad, sanitarias, de suministro de energía o agua, etc.

¿Cómo se podría haber evitado este caso?

La exposición accidental de la base de datos de una app de corredores supone un grave riesgo para la seguridad de sus usuarios. Si la información almacenada hubiera estado cifrada, incluso si terceros accedieran a la base de datos, no podría ser **interpretada** sin la clave. Además, aplicar técnicas de anonimización más estrictas, como la eliminación de patrones de ruta únicos, minimizaría el riesgo de que alguien identifique y rastree a corredores. Implementar **controles de acceso** más seguros y restringir la visibilidad de datos sensibles también contribuiría a evitar situaciones que comprometan la privacidad y seguridad de los usuarios.

[6] Puede saber más sobre los datos genéticos y la asociación con el RGPD en el documento La investigación científica con datos personales genéticos y datos relativos a la salud: perspectiva europea ante el desafío globalizado'

H. DISPOSITIVO ROBADO: DIVULGACIÓN DE DATOS SENSIBLES Y CONFIDENCIALES EN INTERNET

Una asociación que brinda apoyo a personas en proceso de rehabilitación de adicciones sufre un robo en su sede, en el que varios ordenadores, sin protección alguna, son sustraídos. En estos dispositivos se almacenaban datos confidenciales de los usuarios, incluyendo fotografías, historiales médicos, direcciones, teléfonos de contacto y evaluaciones psícologicas. Posteriormente, algunos de estos datos aparecen en foros de Internet, exponiendo a los afectados a discriminación, pérdida de empleo e incluso chantajes.

¿Podría haberse minimizado el impacto si los dispositivos robados estuvieran protegidos?

Si los ordenadores hubieran contado con cifrado de disco completo[7], habría sido más complicado acceder a los archivos sin la clave de descifrado. Además, un sistema de autenticación robusto podría haber impedido el acceso incluso si lograban encender los dispositivos. También, la implementación de soluciones de borrado remoto habría permitido eliminar la información tras el robo. Estas medidas no deben limitarse únicamente a ordenadores portátiles, sino también a todos los dispositivos utilizados.

¿Qué consecuencias podría tener la filtración de estos datos para los afectados?

Los participantes en los programas de la asociación podrían enfrentar graves problemas, incluyendo discriminación en el ámbito laboral, social y familiar. Además, la filtración de sus direcciones y teléfonos los expone a posibles amenazas, chantajes o violencia. En algunos casos, esta información podría ser utilizada por redes criminales para coaccionar a los afectados o forzarlos a situaciones de riesgo.

¿Cómo se podría haber evitado este caso?

La filtración de datos de las personas auxiliadas podría haberse prevenido con un enfoque integral de seguridad de la información. La asociación debería haber implementado **cifrado** en todos los dispositivos para impedir el acceso a los datos por parte de terceros ajenos a la organización sin permiso de acceso a aquellos. Además, el uso de **autenticación de múltiples factores y accesos restringidos** hubiera garantizado que solo el personal autorizado pudiera acceder a la información. Otras medidas esenciales incluyen **políticas de seguridad física**, como la instalación de alarmas, cámaras y cerraduras reforzadas, así como la capacitación del personal en **buenas prácticas de ciberseguridad**.

Contar con una estrategia de **borrado remoto y copias de seguridad cifradas** habría permitido mitigar el impacto en caso de robo, protegiendo a las personas afectas.

[7] El establecimiento de usuario y contraseña para el acceso a un equipo no equivale a cifrar el dispositivo, son medidas complementarias.

III. SI SE CIFRAN LOS DATOS, ¿NO HAY QUE HACER NADA MÁS?

El cifrado es una herramienta fundamental para la protección de datos personales, ya que tiene por objeto que solo las personas autorizadas puedan acceder a información protegida, como bases de datos con nombres y direcciones. También ayuda a preservar la integridad de documentos digitales frente a manipulaciones y a restringir el acceso no autorizado a información sensible, como historiales médicos o datos financieros. En casos de brechas de datos personales, y siempre que el proceso de cifrado y gestión de claves se haya realizado apropiadamente[8], utilizar esta técnica demostraría diligencia por parte del responsable del tratamiento[9], y lo que es realmente importante, reduciría el impacto a las personas afectadas. La eficacia del cifrado depende de la fortaleza de las técnicas y protocolos empleados. Serían requisitos mínimos la adopción de estándares seguros y robustos, como AES-256 para el cifrado de datos y TLS 1.2 o superior para proteger las comunicaciones, así como revisar periódicamente que no se usan algoritmos o claves obsoletos.

Para garantizar la robustez del cifrado, es decir, un nivel de seguridad y protección de los datos adecuados, se recomienda emplear algoritmos y estándares reconocidos como seguros, como el estándar AES con claves de al menos 256 bits (AES-256) para el cifrado de datos, y TLS en versiones iguales o superiores la 1.2 para proteger las comunicaciones. Las técnicas y protocolos criptográficos evolucionan con el tiempo; por ello, es importante revisar periódicamente las configuraciones de seguridad y evitar el uso de algoritmos o claves obsoletos e inseguros.

Sin embargo, el cifrado por sí solo no es una solución definitiva al cumplimiento de la normativa de protección de datos, ya que no garantiza la **privacidad**, tampoco la confidencialidad, ni equivale a la **anonimización** de los datos. El hecho de que una persona tenga acceso a tus datos personales o conozca información sobre ti más allá de lo estrictamente necesario puede afectar tu privacidad, incluso si los datos están protegidos con cifrado. Sin embargo, es una práctica diligente que puede aminorar la responsabilidad en caso de haberla aplicado correctamente.

En cuanto a la anonimización, el cifrado no elimina la relación entre los datos y las personas, ya que sigue existiendo un vínculo identificativo. Para que los datos sean verdaderamente anónimos, es necesario eliminar o disociar cualquier conexión con la identidad de las personas. Además, el proceso de descifrado para realizar operaciones autorizadas implica que los datos pueden ser tratados nuevamente. Si las claves utilizadas se ven comprometidas, por filtración o deducción, o los datos se descifran de manera indebida, la información quedaría expuesta, con todas las implicaciones personales, legales y éticas que ello conlleva.

Los datos personales cifrados continúan siendo datos personales

[8] Ver las Orientaciones para la validación de sistemas criptográficos en la protección de datos y la herramienta asociada Valida-Cripto RGPD

[9] Con relación al cumplimiento del principio de responsabilidad proactiva establecido en el art.5.2 del RGPD

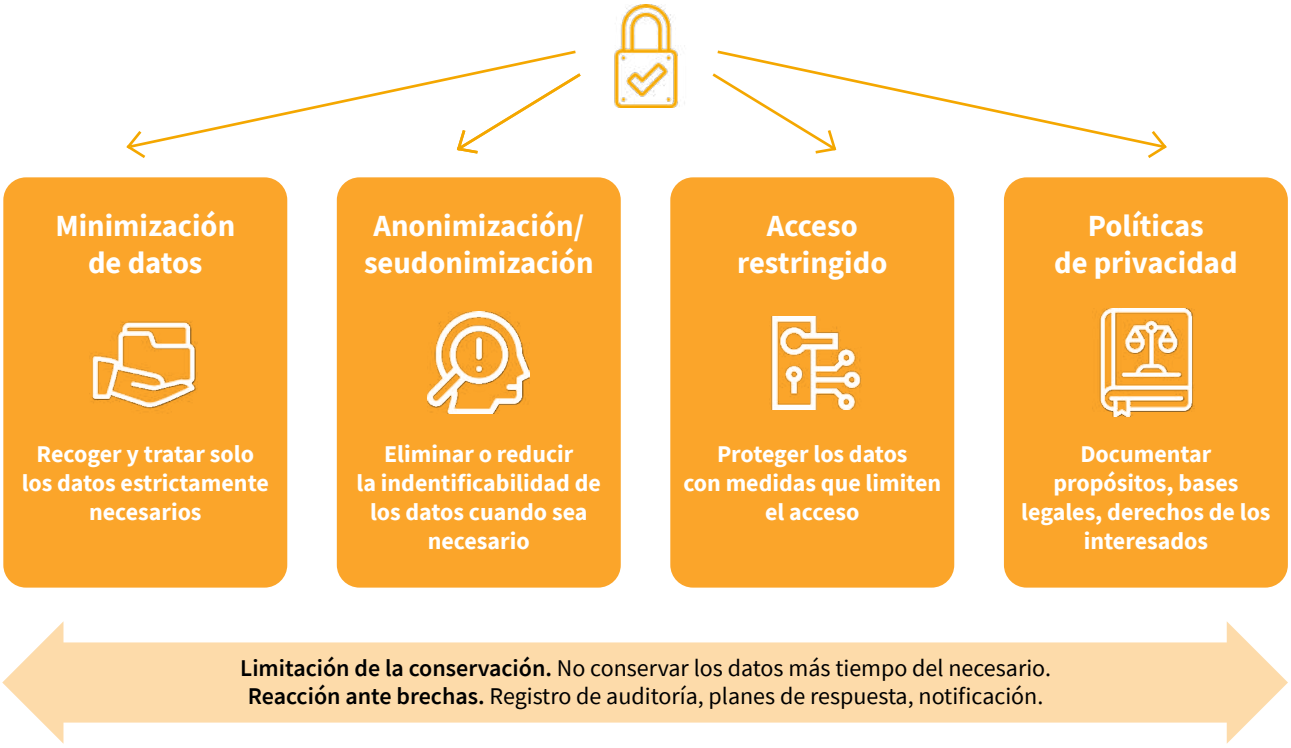
Por esta razón, el cifrado debe integrarse dentro de una estrategia más amplia de privacidad que combine técnicas de minimización, limitación de la conservación, control de accesos, registros de auditoría y procedimientos de reacción ante brechas de datos personales orientados a proteger a los individuos y la sociedad. Como explica la entrada del blog de la AEPD, Cifrado y Privacidad: cifrado en el RGPD, el cifrado es una medida poderosa, pero no suficiente por sí sola para garantizar un tratamiento adecuado de los datos. De hecho, la guía 10 Malentendidos relacionados con la anonimización destaca en su equívoco No. 2 que el cifrado no sustituye la anonimización, ya que no rompe el vínculo entre los datos y las personas.

Por todo ello, la aplicación de los principios y obligaciones que se derivan de la normativa de protección de los datos no depende únicamente del cifrado, sino de la aplicación de un conjunto de buenas prácticas de privacidad en los ámbitos de gestión, legal y técnico. Entre estas medidas se incluyen la minimización de datos en las distintas operaciones de tratamiento, la anonimización cuando sea necesaria, protocolos de acceso restringido y políticas de privacidad adecuadas.

La combinación de estas estrategias permite garantizar que los datos estén protegidos en todas las etapas de su tratamiento y almacenamiento.

ESTRATEGIA DE PRIVACIDAD: MÁS ALLÁ DEL CIFRADO

El cifrado es una técnica útil, pero no suficiente por sí sola. Para cumplir con una normativa de protección de datos, debe integrarse en un marco más amplio de buenas prácticas de privacidad



IV. CÓMO SE PUEDEN CIFRAR LAS COMUNICACIONES

A. NAVEGACIÓN WEB

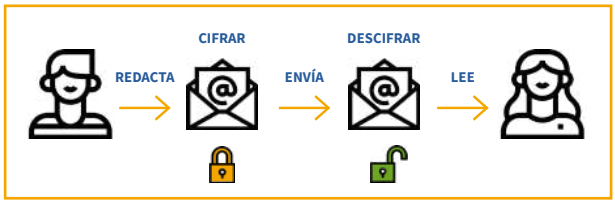
La navegación web es el proceso de acceder a sitios de internet para buscar información o realizar actividades en línea. Para los autónomos y PYMES, es esencial tener precaución al navegar, ya que muchos sitios pueden ser vulnerables a ciberataques que intentan robar información o infectar los dispositivos con software malicioso o malware. Utilizar conexiones seguras (https) y estar atentos a sitios sospechosos es clave para proteger la seguridad en línea. El cifrado ayuda a asegurar que las comunicaciones, aunque sean interceptadas por un tercero, no les sirvan de nada al no poder conocer el contenido.

Si quiere saber más sobre el funcionamiento de los **certificados electrónicos en web**, puede consultar la siguiente información:

- Si tu web cuenta con certificado de seguridad, comprueba que utilizas una versión segura del protocolo TLS | Empresas | INCIBE
- Cifrado de la información | Ciudadanía | INCIBE

B. CORREO ELECTRÓNICO

El correo electrónico es una herramienta fundamental en el día a día de cualquier autónomo o PYME, tanto para la comunicación con clientes como para la gestión interna. Sin embargo, los correos pueden ser una vía de ataque si no se toman las precauciones adecuadas. Para proteger los datos enviados, es importante cifrar los correos electrónicos. Esto garantiza que solo el destinatario pueda leer el mensaje, evitando que personas no autorizadas tengan acceso a información sensible[10]. Además, el uso de contraseñas fuertes y la verificación en dos pasos aumentan la seguridad[11].



Si quiere saber más sobre el **cifrado de los correos electrónicos**, puede consultar la siguiente información:

- Cifrado seguro de correo electrónico con PGP | INCIBE-CERT | INCIBE
- Información sobre el cifrado de correo en Gmail - Ayuda de Gmail

[10] Existen también métodos de autenticación complementarios al cifrado de correos electrónicos que permiten evitar SPAM, ataques de Phishing y otros riesgos de seguridad. Los proveedores de servicios de correo electrónico deben facilitar las medidas de seguridad adecuadas configuradas por defecto, incluyendo información suficiente para que puedan ser utilizados correctamente, así como información clara y precisa de los riesgos que supone desactivar estas medidas de seguridad. Por otro lado, Autónomos y PYMES están obligados a contratar servicios que garanticen estas medidas de seguridad. Puede ampliar la información aquí: Tecnología y formación para proteger tu dominio de correo electrónico | Empresas | INCIBE

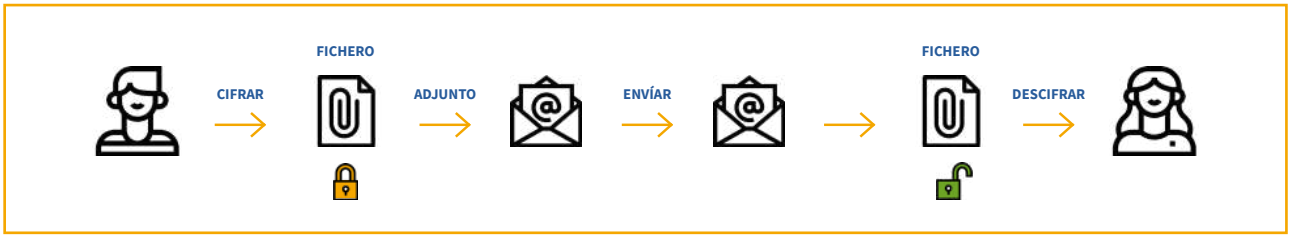
[11] Puede saber más sobre la verificación en dos pasos (2FA) con los siguientes recursos: Cómo utilizar la verificación en dos pasos con su cuenta de Microsoft - Soporte técnico de Microsoft y Cómo activar la Verificación en 2 pasos - Computadora - Ayuda de Cuenta de Google

C. FICHEROS ADJUNTOS

Los ficheros adjuntos son comúnmente utilizados para compartir documentos, presentaciones, contratos u otros archivos importantes. Sin embargo, los archivos adjuntos pueden ser un riesgo de seguridad, ya que pueden contener malware o virus. Para proteger la información, es recomendable cifrar los ficheros antes de enviarlos por correo electrónico o compartirlos a través de plataformas de mensajería. El cifrado asegura que, aunque un archivo sea interceptado, solo aquellos con la clave adecuada puedan abrirlo y acceder a su contenido.

Si quiere saber más sobre el **cifrado de los ficheros para ser adjuntados**, puede consultar la siguiente información:

- Cifrado y almacenamiento seguro de ficheros paso a paso | Ciudadanía | INCIBE
- Soporte WinRAR - Como proteger un archivo con contraseña
- Proteger los datos en un archivo 7zip
- Cómo cifrar sus archivos con WinZip

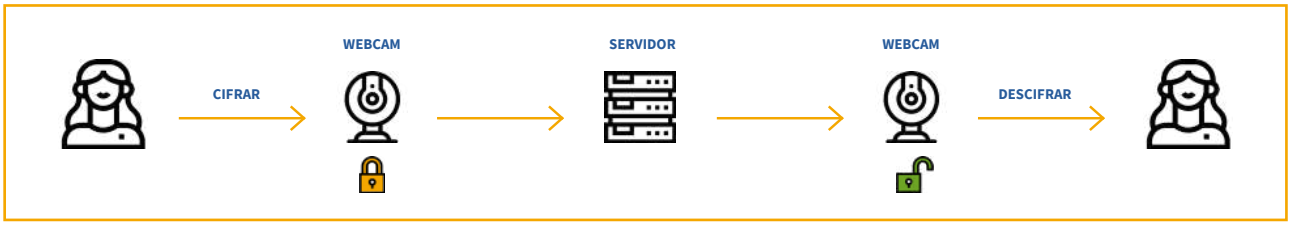


D. VIDEOCONFERENCIAS

Las videoconferencias son una herramienta crucial para la comunicación entre equipos de trabajo o con clientes. Sin embargo, las conversaciones pueden ser vulnerables si no se utilizan plataformas seguras. Es fundamental cifrar las videoconferencias para proteger la privacidad de las reuniones y la información compartida durante las mismas. Al hacerlo, se evita que personas no autorizadas puedan acceder a las conversaciones, lo que es esencial cuando se manejan datos confidenciales o discusiones sensibles.

Si quiere saber más sobre el **cifrado de videoconferencias**, puede consultar la siguiente información:

- Cifrado de un extremo a otro para Microsoft Teams - Microsoft Teams | Microsoft Learn

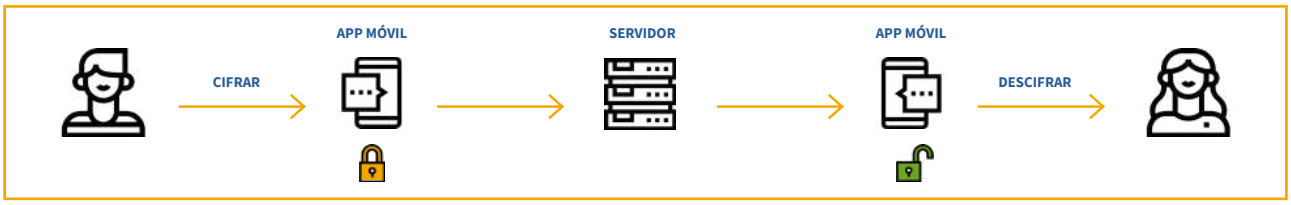


E. APPS DE MENSAJERÍA

Las apps de mensajería se han convertido en una herramienta diaria para la comunicación rápida y efectiva. No obstante, estas aplicaciones pueden ser vulnerables si no se usan adecuadamente. El cifrado de extremo a extremo es crucial para asegurar que los mensajes no puedan ser interceptados por terceros durante el envío. Es importante elegir aplicaciones de mensajería que ofrezcan este nivel de seguridad, protegiendo así la información confidencial y evitando posibles filtraciones de datos.

Si quiere saber más sobre el **cifrado de las apps de mensajería**, puede consultar la siguiente información:

- Cifrado de la información | Ciudadanía | INCIBE
- Información acerca del cifrado de extremo a extremo | Servicio de ayuda de WhatsApp



V. ¿CÓMO SE PUEDEN CIFRAR LOS DATOS ALMACENADOS?

A. FICHEROS

Los ficheros son una de las formas más comunes de almacenar y compartir información en cualquier negocio. Pueden contener desde contratos hasta informes financieros. Es fundamental cifrar los ficheros, especialmente cuando contienen datos sensibles como información personal de clientes o datos financieros. El cifrado garantiza que, aunque un archivo sea robado o interceptado, no podrá ser leído sin la clave adecuada. Implementar medidas de cifrado tanto para archivos almacenados localmente como para los que se comparten a través de internet es una de las mejores formas de proteger la información.

Si quiere saber más sobre el **cifrado de ficheros**, puede consultar la siguiente información:

- Cifrado y almacenamiento seguro de ficheros paso a paso | Ciudadanía | INCIBE
- Proteger un documento con una contraseña Soporte técnico de Microsoft

B. DISCO DURO DE UN ORDENADOR

El disco duro de un ordenador es el espacio donde se almacenan todos los archivos, programas y datos del equipo. Si no está protegido, cualquier persona que tenga acceso al dispositivo puede obtener información valiosa. Cifrar el disco duro es una de las medidas más eficaces para proteger la información almacenada. Al cifrar el disco duro, incluso si el dispositivo es robado o extraviado, el acceso a los datos sería significativamente más difícil sin la clave de descifrado. Cifrar los discos duros de todos los dispositivos empleados es esencial para evitar la fuga de datos confidenciales. Si quiere saber más sobre el **cifrado del disco duro de un ordenador**, puede consultar la siguiente información:

- Recomendaciones en el uso de dispositivos fuera de entornos | CCN
- Unidades de disco duro cifradas | Microsoft Learn

C. DATOS EN LA NUBE

Los datos en la nube son cada vez más comunes en los negocios, ya que permiten almacenar y acceder a la información desde cualquier lugar. Sin embargo, los servicios en la nube también pueden ser vulnerables a ataques. El cifrado de los datos en la nube asegura que, aunque se acceda a los archivos desde un servidor remoto, la información estará protegida. Este cifrado puede aplicarse tanto antes de subir los archivos a la nube como durante el proceso de almacenamiento.

Es importante elegir proveedores de nube que ofrezcan cifrado y aplicar sus propias medidas de protección, como cifrar los archivos sensibles antes de almacenarlos.

Si quiere saber más sobre el **cifrado de datos en la nube**, puede consultar la siguiente información:

- Empezar a utilizar archivos cifrados en Drive, Documentos, Hojas de cálculo y Presentaciones - Android - Ayuda de Google Drive
- Protección de los datos mediante el cifrado - Amazon Simple Storage Service

D. TELÉFONOS MÓVILES

Los teléfonos móviles son una herramienta fundamental para los autónomos y empleados de PYMES, ya que se utilizan tanto para la comunicación como para acceder a la información de la empresa. Sin embargo, los dispositivos móviles son susceptibles a robos o accesos no autorizados. Cifrar el contenido de los teléfonos móviles es esencial para proteger la información que contienen, como correos electrónicos, documentos y contactos.

Además, al cifrar los teléfonos, se asegura que, si el dispositivo se pierde o es robado, los datos personales y profesionales estarán protegidos, evitando el acceso no autorizado a información confidencial.

Si quiere saber más sobre el **cifrado de los teléfonos móviles**, puede consultar la siguiente información:

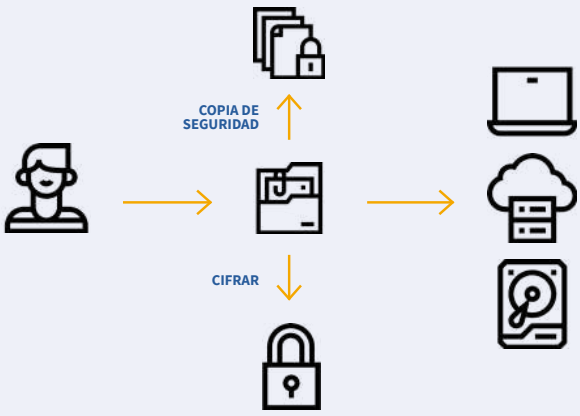
- Cifrado de la información | Ciudadanía | INCIBE
- Cifrado del dispositivo Android: Microsoft Intune | Microsoft Learn
- Utilizar un código con el iPhone, iPad o iPod touch - Soporte técnico de Apple (ES)

E. COPIAS DE SEGURIDAD

Las copias de seguridad son duplicados de los ficheros, documentos y cualquier tipo de información almacenada para conservarlos en otro soporte o ubicación. Son esenciales para garantizar la continuidad del negocio y la recuperación de datos ante incidentes como pérdidas de información, ataques de ransomware o fallos del sistema. Dado que pueden contener información sensible, deben protegerse con el mismo nivel de seguridad que los datos originales tanto si se almacenan localmente como en la nube.

El cifrado de las copias de seguridad es una medida fundamental que impide el acceso no autorizado a la información almacenada, ya sea en discos duros, cintas u otros dispositivos, o en servicios en la nube. Además, es importante auditar el acceso a las claves de cifrado utilizadas para estas copias y controlar los procesos de restauración, asegurando que solo personal autorizado pueda realizarlos. Si quiere saber más sobre el **cifrado de copias de seguridad**, puede consultar la siguiente información:

- Copias de seguridad: una guía de aproximación para el empresario | Empresas | INCIBE
- Copias de seguridad: Políticas de seguridad para la Pyme | Herramientas | INCIBE



VI. PARA SABER MÁS SOBRE LA CRIPTOGRAFÍA

La **criptografía** sirve para proteger la confidencialidad, integridad y autenticidad de la información, impidiendo[12] que personas no autorizadas accedan a ella o la manipulen.

Mediante técnicas de cifrado, los datos se transforman en un formato aparentemente ilegible que solo puede ser descifrado con la clave adecuada, reduciendo el riesgo de robos, fraudes o filtraciones.

Su uso es fundamental en comunicaciones, transacciones digitales y almacenamiento de información sensible, garantizando seguridad y cumplimiento de normativas de protección de datos.

A. ¿QUÉ ES LA CRIPTOGRAFÍA?

La criptografía es la disciplina que se encarga de proteger la información mediante el uso de técnicas matemáticas y algoritmos para convertir datos legibles (texto claro) en un formato cifrado (texto cifrado), que, en principio, solo puede ser entendido por aquellos que poseen las claves necesarias para descifrarlo.

Su objetivo principal es garantizar la seguridad de la información a través de **cuatro pilares** fundamentales:

1. **Confidencialidad:** Asegura que solo las personas autorizadas puedan acceder a los datos.
2. **Integridad:** Garantiza que la información no sea alterada o manipulada durante su almacenamiento o transmisión.
3. **Autenticación:** Verifica la identidad de las partes involucradas en la comunicación o acceso a los datos.
4. **No repudio:** Previene que alguien niegue haber realizado una acción, como enviar un mensaje o realizar una transacción.

En términos básicos, la criptografía transforma un mensaje legible (texto claro) en un mensaje cifrado (texto cifrado) mediante una clave y un algoritmo de cifrado. Solo quien tenga la clave correcta podrá descifrar el mensaje y leerlo. Esto asegura que la información sea segura incluso si es interceptada por terceros no autorizados.

[12] Impidiendo de forma general, ya que no hay una garantía de que, con la información, el tiempo y los recursos necesarios, sea imposible acceder a la información. Por lo tanto, da un grado de confianza que es muy importante, pero no absoluto.

B. CONCEPTOS BÁSICOS

1. **Texto claro (mensaje original):** La información que se quiere proteger.

2. **Texto cifrado:** El mensaje transformado en un formato ilegible para los demás.

3. **Clave:** Una serie de caracteres o números que se utiliza para cifrar o descifrar el mensaje.

4. **Cifrado:** El proceso de transformar el texto claro en texto cifrado. Para garantizar la robustez del cifrado, es decir, un nivel de seguridad y protección de los datos adecuados, se recomienda, al menos, emplear algoritmos y estándares reconocidos como seguros, como el estándar AES con claves de al menos 256 bits (AES-256) para el cifrado de datos, y TLS en versiones iguales o superiores la 1.2 para proteger las comunicaciones. Las técnicas y protocolos criptográficos evolucionan con el tiempo; por ello, es importante revisar periódicamente las configuraciones de seguridad y evitar el uso de algoritmos o claves obsoletos e inseguros.

5. **Descifrado:** El proceso inverso, que convierte el texto cifrado de nuevo a texto claro.

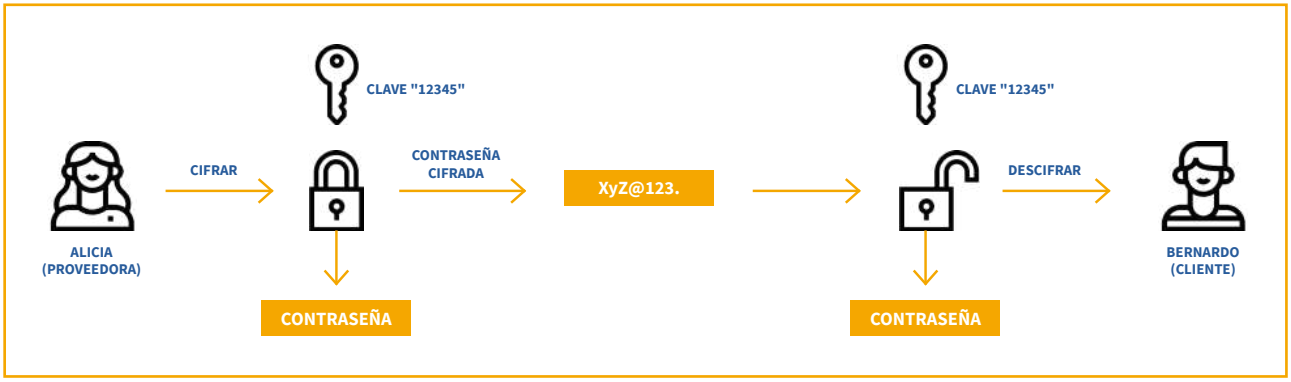
C. EJEMPLO SENCILLO: ALICIA (PROVEEDORA) Y BERNARDO (CLIENTE)

1. **Cifrado:** Alicia quiere enviar a Bernardo una contraseña para que acceda a sus servicios. En lugar de enviarla directamente, la cifra usando una clave (por ejemplo, “12345”) y un algoritmo simple. El mensaje claro, “contraseña”, se convierte en texto cifrado, por ejemplo, XyZ@123.

2. **Transmisión:** Alicia envía el texto cifrado a Bernardo a través de un canal inseguro, como un correo electrónico.

3. **Descifrado:** Bernardo, que conoce la clave “12345”, usa el mismo algoritmo para descifrar el mensaje y obtener la contraseña original.

En la guía Orientaciones para la validación de sistemas criptográficos en la protección de datos publicada por la AEPD, se detallan los elementos que es recomendable evaluar en el diseño y validación de un sistema de cifrado empleado en un tratamiento de datos personales. Estas orientaciones tienen en cuenta la transcendencia del cifrado en dicho tratamiento, especialmente en aquellos casos en el que el cifrado se emplea para preservar la confidencialidad.



Nota: En este ejemplo la clave para cifrar y descifrar el mensaje es la misma, pero esto puede no ser siempre así (cifrado asimétrico).

La guía propone una lista de controles, no exhaustiva ni exigible en su totalidad, para facilitar al responsable o encargado RGPD del tratamiento, al responsable funcional dentro de estas entidades, al DPD, a los asesores en protección de datos y a auditores internos y externos, la selección, validación y supervisión de los sistemas de cifrado en el marco de un tratamiento específico, como parte de las labores de privacidad desde el diseño y responsabilidad proactiva. La herramienta ValidaCripto RGPD permite una aplicación sencilla y práctica de las orientaciones incluidas en la guía, facilitando la evaluación de los sistemas criptográficos en el ámbito del cumplimiento normativo.

VII. RECOMENDACIONES GENERALES

Para mejorar la seguridad de la información y prevenir incidentes como los mencionados, se recomienda adoptar las siguientes prácticas:

1. **Aplicar el principio de minimización de datos.** Solo se debe recopilar, procesar y almacenar la información estrictamente necesaria para cada finalidad. Reducir la cantidad de datos tratados disminuye el riesgo de exposición en caso de brechas de seguridad.

2. **Cifrar los ficheros sensibles antes de enviarlos por correo electrónico o almacenarlos en la nube**. Esto garantiza que, aunque un archivo sea interceptado, no podrá ser leído sin la clave para descifrarlo.

3. **Enviar la clave de descifrado por un canal separado del archivo cifrado.** Para evitar que un atacante que intercepte el mensaje pueda acceder a la información protegida, la clave nunca debe enviarse en el mismo correo o plataforma que el archivo cifrado.

4. **Cifrar el disco duro de los dispositivos utilizados para gestionar información confidencial.** En caso de robo o extravío, los datos permanecerán inaccesibles sin la clave pertinente.

5. **Utilizar servicios de correo electrónico con cifrado y herramientas seguras para el intercambio de documentos.** Priorizar plataformas que ofrezcan cifrado de extremo a extremo para garantizar la protección de los datos.

6. **Habilitar la autenticación en dos pasos en cuentas de correo, plataformas de almacenamiento en la nube y otros servicios críticos** para reducir el riesgo de accesos no autorizados.

7. **Ser cuidadoso al compartir información sensible, revisando los destinatarios antes de enviar correos o mensajes con archivos confidenciales.** Aplicar restricciones de acceso a documentos compartidos puede evitar filtraciones accidentales.

8. **Evitar incluir en el asunto del correo información que pueda revelar datos sensibles o dar pistas sobre el contenido del mensaje.** Esto incluye referencias explícitas a datos personales, diagnósticos, transacciones o posibles claves para descifrar el contenido.

9. **Utilizar aplicaciones de mensajería con cifrado de extremo a extremo cuando se transmitan datos sensibles.** Esto impide que terceros intercepten y accedan a la información.

10 **Realizar copias de seguridad cifradas de la información importante en dispositivos y en la nube.** Esto garantiza la disponibilidad de los datos sin comprometer su seguridad en caso de incidentes.

11 **Implementar controles de acceso y permisos basados en roles.** Limitar el acceso a la información únicamente a las personas que realmente lo necesiten dentro de una organización reduce significativamente el riesgo de filtraciones.

12 **Capacitar y concienciar al personal sobre la protección de datos.** Muchas brechas de seguridad ocurren por errores humanos. Formación periódica en ciberseguridad y buenas prácticas en el manejo de información confidencial ayuda a prevenir incidentes.

Como recomendación final, al igual que autónomos y PYMES recurren a especialistas para instalar sus sistemas de alarmas, gestionar sus deberes contables, fiscales o de contratación, instalar su electricidad, fontanería o mecánica, etc, **aconsejamos que recurran a especialistas de privacidad y seguridad cuando lo necesiten.**

Implementando estas medidas, autónomos y PYMES pueden fortalecer la protección de la información, minimizando el impacto de errores humanos, accesos no autorizados y ciberataques.

VIII. REFERENCIAS Y ANEXOS

REFERENCIAS

- Parlamento Europeo y Consejo de la Unión Europea. (2016). **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). Diario Oficial de la Unión Europea. VER REFERENCIA
- Agencia Española de Protección de Datos (AEPD). (2021). **Cómo comunicar una brecha de datos personales**. VER REFERENCIA
- Agencia Española de Protección de Datos (AEPD). (2022). **La AEPD publica una guía dirigida a profesionales del sector sanitario.** VER REFERENCIA
- Agencia Española de Protección de Datos (AEPD). (2025). **Notificación de brechas de datos personales a la Autoridad de Control.** VER REFERENCIA
- Agencia Española de Protección de Datos (AEPD). (2019). **Cifrado y Privacidad: cifrado en el RGPD.** VER REFERENCIA
- Agencia Española de Protección de Datos (AEPD). (2020). **Cifrado y Privacidad II: El tiempo de vida del dato.** VER REFERENCIA

- Instituto Nacional de Ciberseguridad (INCIBE). (2020). **El ataque del "man in the middle" en la empresa: riesgos y formas de evitarlo.** VER REFERENCIA
- Instituto Nacional de Ciberseguridad (INCIBE). (2018). **Cifrado seguro de correo electrónico con PGP.** VER REFERENCIA
- PassFab. (2025). **Cómo desbloquear un archivo de Excel protegido.** VER REFERENCIA
- Information Commissioner's Office (ICO). (2025). **Encryption scenarios.** VER REFERENCIA
- National Cyber Security Centre (NCSC). (2025). **Cyber Aware.** VER REFERENCIA
- National Institute of Standards and Technology (NIST). (2020). **Cybersecurity Basics - Case Study Series.** VER REFERENCIA
- Commission Nationale de l'Informatique et des Libertés (CNIL). (2021). **Violation du trimestre: les attaques sur les messageries.** VER REFERENCIA
- Commission Nationale de l'Informatique et des Libertés (CNIL). (2011). **Comment réagir face à une usurpation d'identité.** VER REFERENCIA

ANEXOS

- Agencia Española de Protección de Datos (AEPD). (2016). **Guía de privacidad y seguridad en Internet.** VER ANEXO
- Agencia Española de Protección de Datos (AEPD). (2020). **Guía sobre protección de datos por defecto.** VER ANEXO
- Agencia Española de Protección de Datos (AEPD). (2019). **Guía de privacidad desde el diseño.** VER ANEXO
- Agencia Española de Protección de Datos (AEPD). (2021). **Gestión del riesgo y evaluación de impacto en tratamientos de datos personales.** VER ANEXO
- Agencia Española de Protección de Datos (AEPD). (2020). **Listado de medidas de protección de datos por diseño y por defecto.** VER ANEXO
- Agencia Española de Protección de Datos (AEPD). (2020). **Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo.** VER ANEXO
- Agencia Española de Protección de Datos (AEPD). (2023). **Orientaciones para la validación de sistemas criptográficos en la protección de datos.** VER ANEXO
- Agencia Española de Protección de Datos (AEPD). (2024). **Hoja de ruta para garantizar la conformidad con la normativa de protección de datos.** VER ANEXO

www.aepd.es

@aepd_es aepd.es @AEPD_es aepd-es