IdiPAZ+i News

Nº 18

Octubre 2022

BOLETÍN DE INFORMACIÓN CIENTÍFICA E INNOVACIÓN DEL IDIPAZ

IdiPAZ/FIBHULP ha implementado todas las medidas para garantizar el cumplimiento de la normativa existente en materia de protección de datos

De acuerdo con la legislación existente en materia de protección de datos y de cara a garantizar su cumplimiento, se enviaron a las Unidades y Plataformas de Apoyo de IdiPAZ una serie de medidas a implantar, con el fin de preservar la seguridad de la información que se maneja dentro del entorno de investigación del IdiPAZ.

Se comunicó cómo se debe proceder en la relación con los proveedores (aquellas empresas o autónomos que nos prestan algún servicio) con los que se interactúa habitualmente.

En ese sentido, en el caso de que se esté trabajando con algún proveedor o se haga de cara a un futuro próximo y que trate datos personales por cuenta de la FIBHULP, es decir, que utilice de alguna manera datos que sean propiedad de la Fundación, deberá ser evaluado como nuevo encargado de tratamiento, ya que se dedicará a cumplir las órdenes dadas por la FIBHULP en cuanto a materia de protección de datos, para lo que se les deberá enviar el cuestionario de evaluación para encargados del tratamiento, para que lo devuelvan cumplimentado y firmado. Dicho cuestionario se debe enviar a aquellos encargados de tratamiento sitos dentro y fuera de la Unión Europea. Por otro lado, esta empresa/proveedor, también deberá firmar el correspondiente contrato de encargado del tratamiento con la FIBHULP.

Ambos documentos se pueden solicitar y enviar, una vez que estén cumplimentados, a la siguiente dirección: innovacion.legal@idipaz.es

También se han resaltado las medidas de seguridad a aplicar para el supuesto de que se vaya a llevar a cabo una transferencia de datos de carácter sensible. Estas medidas deberán aplicarse desde el momento de seleccionar qué se envía y a quién, hasta el momento de la correcta recepción y acuse de que la información que se ha facilitado es la correcta.

Todo ello entendiendo que se trata de datos personales en tanto en cuanto puedan hacer identificable a una persona física.

Se ha ampliado el espectro y ahora también se considera como tal, las cookies, las direcciones IP o identificadores de dispositivos móviles, ya que aunque estos datos no están unidos a un nombre, sí pueden permitir identificar a una persona unívocamente.

Medidas de seguridad para la transferencia de datos

De acuerdo con la legislación existente en materia de protección de datos y de cara a garantizar su cumplimiento, en este documento se reflejan las medidas de seguridad que se deben adoptar de forma que se pueda garantizar la confidencialidad, integridad, disponibilidad y resiliencia de la información que se facilite durante todo proceso en el que se lleve a cabo una transferencia de datos de carácter sensible.

Las principales medidas son:

- NO COMUNICAR NI COMPARTIR DATOS PERSONALES POR CORREO ELECTRÓNICO. Existen en el mercado soluciones informáticas más seguras que el correo electrónico.

  Estos son algunos ejemplos de estos servicios de sincronización e intercambio de archivos cifrados que permiten almacenar, sincronizar y compartir documentos confidenciales:

  https://ethical.net/resources/?resource-category=file-sharing) otros ejemplos:
  https://tresorit.com/
  https://nextcloud.com

- Sólo en caso que sea IMPRESCINDIBLE compartirlos por correo electrónico, tener en cuenta lo siguiente:

  1. Realizar el envío a través de cuentas de correo electrónico corporativas, nunca personales. En este sentido, sólo debe estar permitido, de forma excepcional, el envío de datos de investigación por correo electrónico cuando, tanto la cuenta del remitente como la del destinatario, pertenezcan al dominio salud.madrid.org.
  2. No hacer uso de dispositivos (ordenadores, móviles, etc.) personales o no autorizados por la Fundación para realizar los envíos.
  3. Los datos deben enviarse cifrados y protegidos con contraseña. Debe seleccionarse un cifrado adecuado a la categoría de datos que van a ser compartidos: https://www.aepd.es/es/prensa-y-comunicacion/blog/cifrado-y-privacidad-ii-el-tiempo-de-vida-del-dato

4. Evaluar la posibilidad de utilizar el cifrado homomórfico: https://www.aepd.es/es/prensa-y-comunicacion/blog/cifrado-privacidad-iii-cifrado-homomorfico

5. Usar contraseñas de calidad, con longitudes mínimas (p. ejemplo: 10 caracteres), fáciles de recordar, difícilmente adivinables (no incluir nombres, teléfonos, fechas señaladas, palabras incluidas en diccionarios…), con caracteres alfanuméricos.

6. Los datos deben enviarse seudonimizados, eliminándose todo identificador directo e indirecto no necesario (p. ejemplo: indicar rango de edad, en lugar de edad exacta; indicar año de nacimiento, en lugar de fecha de nacimiento). Se debe procurar utilizar técnicas avanzadas de seudonimización:
https://www.aepd.es/sites/default/files/2020-05/estudio-hash-anonimidad.pdf
https://www.aepd.es/sites/default/files/2019-09/nota-tecnica-kanonimidad.pdf
https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases/

7. Enmascaramiento u ofuscación de datos mediante el uso de Privacy Enhancing Technologies "PET" (en la medida que no afecten la calidad el dato y, por tanto, el resultado de la investigación):
https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies

8. Uso de VPN si se realizan los envíos desde fuera de las instalaciones de la FIBHULP/IDIPAZ.

9. Cuando sea posible, los datos transferidos a un dispositivo de almacenamiento portátil deben tener una caducidad, es decir, eliminar la información del correo una vez se ha enviado o se ha recibido, y ya no sea necesario tenerla almacenada en este medio.

10. Disponer de un listado de las personas que pueden realizar estos envíos y autorizarles a hacerlo.

11. Verificación de que el destinatario al que se va a enviar la información es al que se le quiere enviar, especialmente si tenemos en cuenta los incidentes de seguridad que ha experimentado la FIBHULP/IDIPAZ en los últimos meses consecuencia del envío de correos a destinatarios equivocados.

12. No colocar en el título del correo ninguna referencia a que se trata de información confidencial/datos de investigación/cualquier otro título que de pistas sobre la sensibilidad/criticidad del contenido del correo.

13. Uso de la herramienta *GuardedBox* para el envío de contraseñas: se trata de una solución online de código abierto que permite, desde cualquier dispositivo con un navegador web, el almacenamiento, la compartición y el intercambio de contraseñas, entre otros, de manera segura, con cifrado extremo a extremo, gestionando todas las tareas de protección y cifrado de los datos, sin confiar en el servidor, y haciendo uso de las mejores prácticas de la industria de ciberseguridad. La instancia pública de *GuardedBox* es 100% gratuita: https://guardedbox.es/

INSTRUCCIONES DE ENCRIPTADO

Compresión con cifrado de ficheros con el Programa 7-

Si necesitamos enviar por correo electrónico un fichero de datos cifrado, la mejor manera es comprimirlo (para que ocupe menos) con clave compleja: mínimo 10 caracteres alfanuméricos incluyendo símbolos, números y letras, preferiblemente mayúsculas y minúsculas).

Hay un software gratuito y de código abierto, el 7-zip (hay otros, pero de código abierto y gratuitos no tantos) que es fiable y que puede utilizar un sistema avanzado de cifrado, (AES-256, el estándar actual para las comunicaciones seguras sobre internet). En el apartado 2 de este documento, se explica cómo descargar e instalar el software de compresión y cifrado 7-zip.

Una vez instalado como se indica en el segundo punto del documento, se pulsa el botón derecho del ratón sobre el fichero que se desea enviar como adjunto a un correo electrónico; se despliega el menú contextual y de éste se selecciona 7-Zip, que abre un menú secundario y se selecciona "Añadir al archivo…":

Aunque en este ejemplo es un fichero en el escritorio, puede estar en una carpeta abierta con el navegador.

Aparece una ventana de diálogo, en la que hay que establecer o comprobar que esté lo siguiente:

1- Cambiar el nombre de fichero comprimido a uno que no indique la información que contiene y siempre sin datos personales.

2- Establecer el formato de archivo a ".7z" (aparecen otros campos después de esta acción).

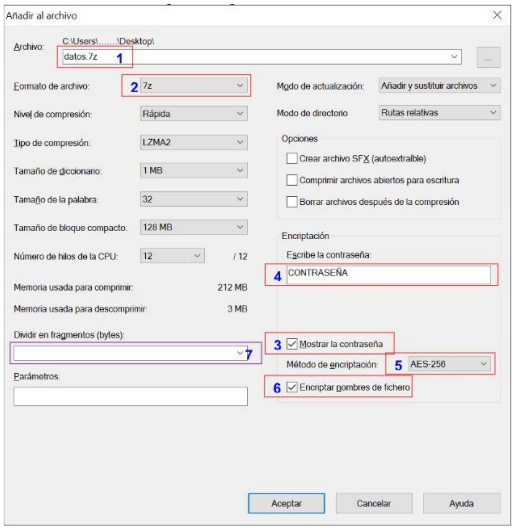
3- Marcar la casilla "Mostrar la contraseña" para asegurarse de que se escribe bien.

4- Escribir la contraseña acordada (aquí se ha puesto contraseña, que evidentemente es horriblemente mala).

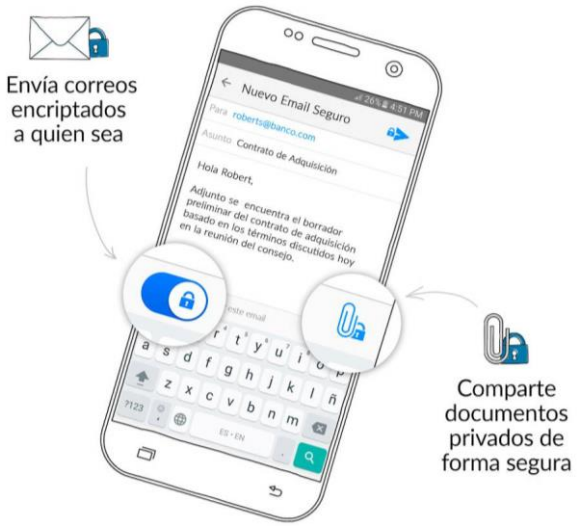
5- Seleccionar como método de cifrado AES-256.

6- Marcar la casilla "Encriptar nombres de fichero", que impide que se puedan analizar los nombres de fichero sin saber la contraseña, y así que se determine su potencial utilidad y si vale la pena intentar romper el cifrado.

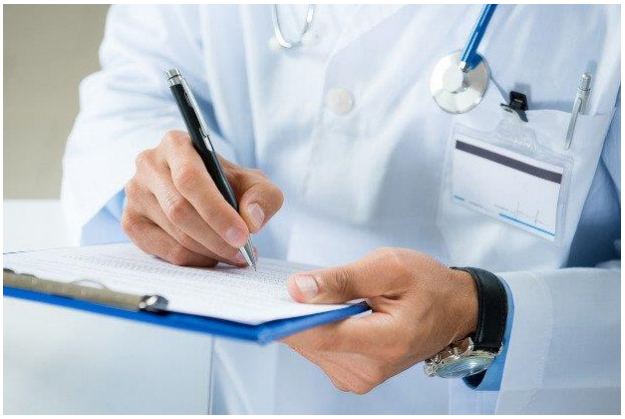
7- Si es necesario, el fichero se puede dividir en fragmentos de 10M, 100M, 1000M… para que se pueda enviar en correos sucesivos si el correo tiene un límite al tamaño del adjunto. Como se muestra en el siguiente diagrama:



Al aceptar, genera un fichero en el directorio donde estaba el fichero origen, de menor tamaño habitualmente y con extensión ".7z" que sólo se puede abrir con la clave introducida. Éste fichero ("7z") es el que se adjunta. NUNCA SE DEBE ENVIAR LA CLAVE POR CORREO ELECTRONICO (NI EN EL MISMO E-MAIL NI EN UN CORREO DIFERENTE). Debe hacerse por audio normal por teléfono (no por mensajería instantánea, como WhatsApp).



IMPORTANTE: recordad que esta solución aquí planteada es una solución temporal hasta que se adquiera una herramienta que permita llevar a cabo estas acciones de forma segura.



AMNESIA, una herramienta para la anonimización de datos.

Herramientas de anonimización de datos.

Todos sabemos que los datos anonimizados desempeñan un papel muy importante en el contexto de la investigación y debemos tener en cuenta, que el deber de todo aquel que trata datos de carácter personal, es velar por la privacidad de los sujetos propietarios de dichos datos.

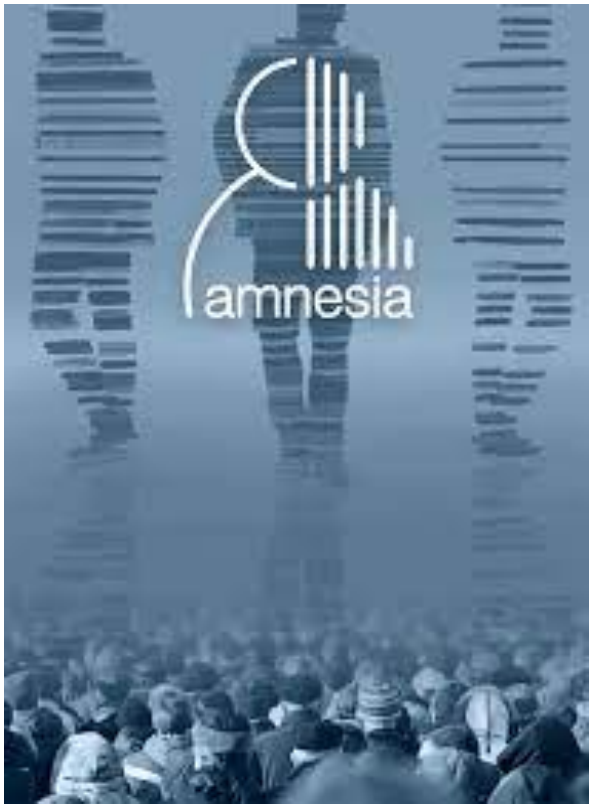
Por ello, de acuerdo con la legislación existente en materia de protección de datos y de cara a garantizar su cumplimiento, os informamos que existe un programa gratuito, a disposición de cualquier investigador, que cumple con la citada finalidad, se denomina **AMNESIA**.

"Amnesia es una de las herramientas más utilizadas para la anonimización de datos. Permite eliminar información de identificación de los datos, siendo flexible y transformando bases de datos relacionales y transaccionales en conjuntos de datos donde se mantienen las garantías formales de privacidad. Es decir, transforma la información no sólo asociada a los identificadores directos como nombres o números de documentos identificativos, sino que también transforma los atributos cuasi-identificadores como la fecha de nacimiento y el código postal para mitigar los riesgos de reidentificación de los sujetos que figuran en las fuentes"

Dispone de una versión online a la que puedes acceder desde el siguiente enlace: https://amnesia.openaire.eu/amnesia/

De acuerdo con ello, es importante señalar que el uso de este tipo de herramientas es fundamental para evitar cualquier tipo de brecha de seguridad, que puede dar lugar a determinadas responsabilidades, no sólo para la institución sino también para el propio investigador.

Cualquier duda o aclaración que necesites sobre dicho programa no dudes en contactar con nuestro responsable de protección de datos, Estela Sánchez innovación.legal@idipaz.es



USO DE LA COPIA OCULTA

De acuerdo con el compromiso asumido por la FIBHULP/IDIPAZ de cumplir con la normativa existente en materia de protección de datos, debemos poner de relieve la importancia de adoptar las medidas de seguridad (técnicas u organizativas) que tengamos a nuestra disposición, para evitar cualquier infracción contenida en el Reglamento General de Protección de Datos (RGPD).

Debemos advertir de la importancia de configurar los correos de forma que se puedan enviar con copia oculta cuando se envíen a varios destinatarios a la vez (cuando se dirija a una pluralidad de interesados).

Recientemente la Agencia Española de Protección de Datos (AEPD) ha sancionado a una entidad por enviar un correo electrónico sin copia oculta a 241 destinatarios, facilitándose así a cada destinatario el acceso al correo electrónico del resto de los destinatarios, entendiendo que los hechos son constitutivos de infracción del Artículo 5.1.f) del RGPD (principio de integridad y confidencialidad) y Artículo 32 del RGPD (seguridad del tratamiento) al revelar información y datos de carácter personal a terceros; todo ello, por no haber hecho uso de la funcionalidad de "con copia oculta CCO".

Podemos extraer que la AEPD considera que, como medida para evitar esta comunicación de datos personales no autorizada vía email, debe procederse al envío de correos con copia oculta cuando se dirija a una pluralidad de interesados.

Os hacemos a continuación, un recordatorio de buenas prácticas en el uso del correo electrónico corporativo:

- Es una herramienta de trabajo, el usuario no hará uso del mismo para fines particulares.
- El usuario comprueba los destinatarios del mensaje (atención función de autocompletado) antes de su envío, utiliza copia oculta en listas de distribución y cuando se envíen comunicaciones a varios destinatarios, elimina direcciones no necesarias para reenvíos.
- No se permite la descarga automática de imágenes
- No se permite el envío de publicidad no solicitada
- No se permite la apertura de ningún correo electrónico de origen no conocido o dudoso. Las acciones a realizar en estos casos son:
  - no interactuar con los enlaces incluidos ni abrir los archivos adjuntos.
  - no proporcionar información.
  - se pondrá en conocimiento del departamento correspondiente establecido para su verificación.
  - se procederá a su eliminación.
  - no se permite la redirección de los mensajes a otro usuario, salvo excepciones autorizada.

Formación en materia de Protección de Datos

La preocupación por la protección de datos está adquiriendo cada vez una importancia mayor para la investigación científica. Además de formar parte de las políticas de responsabilidad social del IdiPAZ, ha sido siempre un aspecto primordial en las investigaciones, los ensayos clínicos y los estudios de *big data* que se llevan a cabo en el IdiPAZ.

Para formar a los investigadores se han elaborado manuales e impartido seminarios formativos:

1. Seminario Científico **"Protección de datos en investigación e innovación"** impartido el 27/10/21 por Dª Natalia Olivares Consultora RGPD, LOPD-GDD en Alaro Avant S.L.
   Enlace al seminario: https://youtu.be/HUvh78mgcBo
   Documentación: "La protección de datos en investigación: aspectos clave a tener en cuenta"

2. CURSO "**Impacto de la normativa de Protección de Datos en los Proyectos de Investigación"** impartido por la Dirección General de Investigación, Docencia y Documentación el pasado mes de marzo con el siguiente: PROGRAMA

Próximos eventos formativos

1. Píldora Formativa REGIC: **Proyectos de investigación y tratamiento de datos personales**
   Fecha: 3 de noviembre de 2022, de 10:00 a 12:00 horas.
   Ponentes: Sarai Nieto y Natalia Olivares, delegadas de Protección de Datos en Alaro Avant.
   Programa
   Inscripciones (Hasta el 28 de octubre)

2. Seminario del Programa Mentor para la preparación de Propuestas AES: **"Plan de gestión de datos científicos y Protección de datos"**
   Fecha: 12 de enero de 2023 a las 9:00 horas
   Ponentes: Daniel Quijada y Estela Sánchez
   Enlace: meet.google.com/wkx-zdwr-niv Unirse por tfno. +34 935 24 96 67 PIN: 987050109

Documentación:

- Manual de Protección de datos
- Registro de actividades de tratamiento de datos de carácter personal
- Medidas de seguridad para la transferencia de datos
- Instrucciones de encriptación

Boletín de Información Científica

Fundación para la Investigación Biomédica del Hospital Universitario La Paz. Edificio Norte, 4ª Planta. 28046. Madrid

Contacto: comunicacion@idipaz.es