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.

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.

Las medidas son las siguientes:

- NO COMUNICAR NI COMPARTIR DATOS DE ESTA CATEGORÍA POR CORREO ELECTRÓNICO. Existen en el mercado soluciones informáticas más seguras que el correo electrónico (https://ethical.net/resources/?resource-category=file-sharing). Por ejemplo:
  - https://nextcloud.com/ y
  - https://tresorit.com/

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

  - 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.
  - No hacer uso de dispositivos (ordenadores, móviles, etc.) personales o no autorizados por la Fundación para realizar los envíos.
  - 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
  - Evaluar la posibilidad de utilizar el cifrado homomórfico: https://www.aepd.es/es/prensa-y-comunicacion/blog/cifrado-privacidad-iii-cifrado-homomorfico
  - 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.
  - 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/
  - 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
  - Uso de VPN si se realizan los envíos desde fuera de las instalaciones de la Fundación.
  - 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 es necesario tenerla almacenada en este medio.
  - Disponer de un listado de las personas que pueden realizar estos envíos y autorizarles a hacerlo.
  - 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 FIB en los últimos meses consecuencia del envío de correos a destinatarios equivocados.
  - 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.

- 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/