PROTOCOLO DE ACTUACIÓN Y SEGURIDAD EN EL TRATAMIENTO DE DATOS PERSONALES E INFORMACIÓN

FUNDACIÓN PARA LA INVESTIGACIÓN DE MÁLAGA EN BIOMEDICINA Y SALUD -FIMABIS-

Instituto de Investigación Biomédica de Málaga y Plataforma en Nanomedicina -IBIMA Plataforma BIONAND-

Ins. Reg. Fund. Consej. Justicia y Administraciones Públicas Junta Andalucía nº MA-606

C.I.F.: G29830643

Calle Severo Ochoa, 35

Parque Tecnológico de Andalucía (PTA) Campanillas, Málaga 29590

tlf. 951 367600; fimabis@fimabis.org / ibima@ibima.eu

FIMABIS

ibima Plataforma BIONAND

Procedimiento Operativo Estandarizado Seguridad (POES)

INFORMACIÓN DE VERSIÓN:

	REALIZADO:	REVISADO:	APROBADO:
FECHA	14/04/2026	**20/04/2026**	**20/04/2026**
NOMBRE Y FIRMA	Jesús López del Peral **Responsable de Sistemas de la Información**	**COMITÉ DE SEGURIDAD DE LA INFORMACIÓN**	**COMITÉ DE SEGURIDAD DE LA INFORMACIÓN**
			
	José Montilla Chicano **Asesor de Protección de Datos y Seguridad de la Información** (externo)		
			

Lugar de archivo: Centauro

Responsables custodia: Eva Pena

Fecha de revisión
20/04/2028

Registro histórico de versiones

VERSIÓN: SEGUNDA	FECHA DE REALIZACIÓN **05/06/2025** **REVISIÓN: 10/09/2025 DPD)**	FECHA DE APROBACIÓN **05/06/2025**

MODIFICACIONES:

1.- Cambio de Domicilio: Parque Tecnológico de Andalucía (PTA)Avenida Severo Ochoa, 35, 29590, Málaga

2.- Delegado de Protección de Datos:

Con fecha 7/6/2024 se ha procedido al nombramiento de Don José Montilla Chicano como DPD de la entidad

VERSIÓN: TERCERA	FECHA DE REALIZACIÓN **20/04/2026**	FECHA DE APROBACIÓN **20/04/2026**

MODIFICACIONES:

Inclusión Anexo F: NORMATIVA DE USO DE MEDIOS ELECTRÓNICOS

CONTENIDO

PREÁMBULO

La protección de los datos personales y seguridad de la información es una necesidad jurídica y organizativa inherente al Estado de Derecho que debe velar por la protección y salvaguarda de los derechos de las personas.

El derecho a la autodeterminación informativa, el reconocimiento de la potestad de la persona sobre sus datos e información es un Derecho Fundamental y su protección exige la concienciación y responsabilidad en el tratamiento de datos de carácter personal, sea este tratamiento realizado en cualquier formato o sistema.

El avance de la tecnología y la globalización de la información, precisan de un ejercicio positivo de protección que se debe dispensar al flujo de informaciones y su tratamiento, tal y como se recoge en el Reglamento Europeo 2016/679 de protección de datos de carácter personal (RGLMEU), y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

Protección de datos desde el diseño y por defecto

*1.**Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, concebidas para aplicar de forma efectiva los principios de protección de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.***

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

A tal fin, se redacta y eleva a compromiso el presente PROTOCOLO

ÍNDICE

BASE LEGAL.

- REGLAMENTO EUROPEO 2016/679 DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL
- LEY ORGÁNICA 3/2018, DE 5 DE DICIEMBRE, DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES.
- REAL DECRETO LEGISLATIVO 2/2015, DE 23 DE OCTUBRE, POR EL QUE SE APRUEBA EL TEXTO REFUNDIDO DE LA LEY DEL ESTATUTO DE LOS TRABAJADORES
- LEY 41/2002, DE 14 DE NOVIEMBRE, BÁSICA REGULADORA DE LA AUTONOMÍA DEL PACIENTE Y DE DERECHOS Y OBLIGACIONES EN MATERIA DE INFORMACIÓN Y DOCUMENTACIÓN CLÍNICA
- LEY 14/2007, DE 3 DE JULIO, DE INVESTIGACIÓN BIOMÉDICA
- REAL DECRETO 1090/2015, DE 4 DE DICIEMBRE, POR EL QUE SE REGULAN LOS ENSAYOS CLÍNICOS CON MEDICAMENTOS, LOS COMITÉS DE ÉTICA DE LA INVESTIGACIÓN CON MEDICAMENTOS Y EL REGISTRO ESPAÑOL DE ESTUDIOS CLÍNICOS

DISPOSICIONES GENERALES, Objeto, Ámbito, Definiciones

1. Objeto. El presente Protocolo tiene por objeto el establecimiento de las buenas prácticas de seguridad en el tratamiento de datos e información de la Entidad.
Se entiende por **PROTECCIÓN DE DATOS E INFORMACIÓN,** el conjunto de principios y normas que tienen por fin establecer de forma ordenada y normada los procedimientos, protocolos, medidas de seguridad e instrumentos para la tutela y garantía del derecho fundamental a la protección de datos personales e información, en su recogida y uso por la **ENTIDAD**.

2. Ámbito. El presente Protocolo será de aplicación a todo tratamiento de la información, ya sea en formato físico o digitalizado, que comprenda información ordenada y sistematizada concerniente a personas físicas, creados o gestionados por la **ENTIDAD**, para el cumplimiento de sus fines y ejercicio de sus competencias.

3. Definiciones. A efectos del RGLMEU y LOPDGDD, se entenderá por:

- Autoridad de control: la autoridad pública independiente establecida por un Estado miembro.
- Autoridad de control interesada: la autoridad de control a la que afecta el tratamiento de datos personales debido a que:
  - el responsable o el encargado del tratamiento esté establecido en el territorio del Estado miembro de esa autoridad de control;
  - los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o/se ha presentado una reclamación ante esa autoridad de control.
- Consentimiento de interesado/a: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado, o interesada, acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.
- Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicos o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.
- Datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.
- Datos personales: toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social en dicha persona.

- Datos relativos a la salud: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.
- Delegado/a de Protección de Datos (DPD o DPO): Al supervisar la observancia interna del presente Reglamento, el/la responsable o el/la encargado/a del tratamiento debe contar con la ayuda de una persona con conocimientos especializados del ámbito del derecho, seguridad informativa y la práctica en materia de protección de datos.
    - Artículo 37. RGPD. Designación del delegado de protección de datos

      1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:
      a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
      b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o
      c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales, (incluidos datos de menores) con arreglo al art. 9 y de datos relativos a condenas e infracciones penales a que se refiere el art. 10.
- Destinatario/a: la persona física o jurídica, autoridad pública, servicio u organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.
- Elaboración de perfiles: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.
- Empresa: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica.
- Encargado del tratamiento o ENCARGADO/A: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.
- Establecimiento principal:
    - en lo que se refiere a un RESPONSABLE del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal.
    - en lo que se refiere a un ENCARGADO del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al Reglamento.
- Fichero: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.
- Grupo empresarial: grupo constituido por una empresa que ejercer el control y sus empresas controladas.
- Limitación del tratamiento: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.
- Normas corporativas vinculantes: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial, o una unión de empresas dedicadas a una actividad económica conjunta.
- Objeción pertinente y motivada: la objeción a una propuesta de decisión sobre la existencia o no de infracción del Reglamento, o sobre la conformidad con el Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los

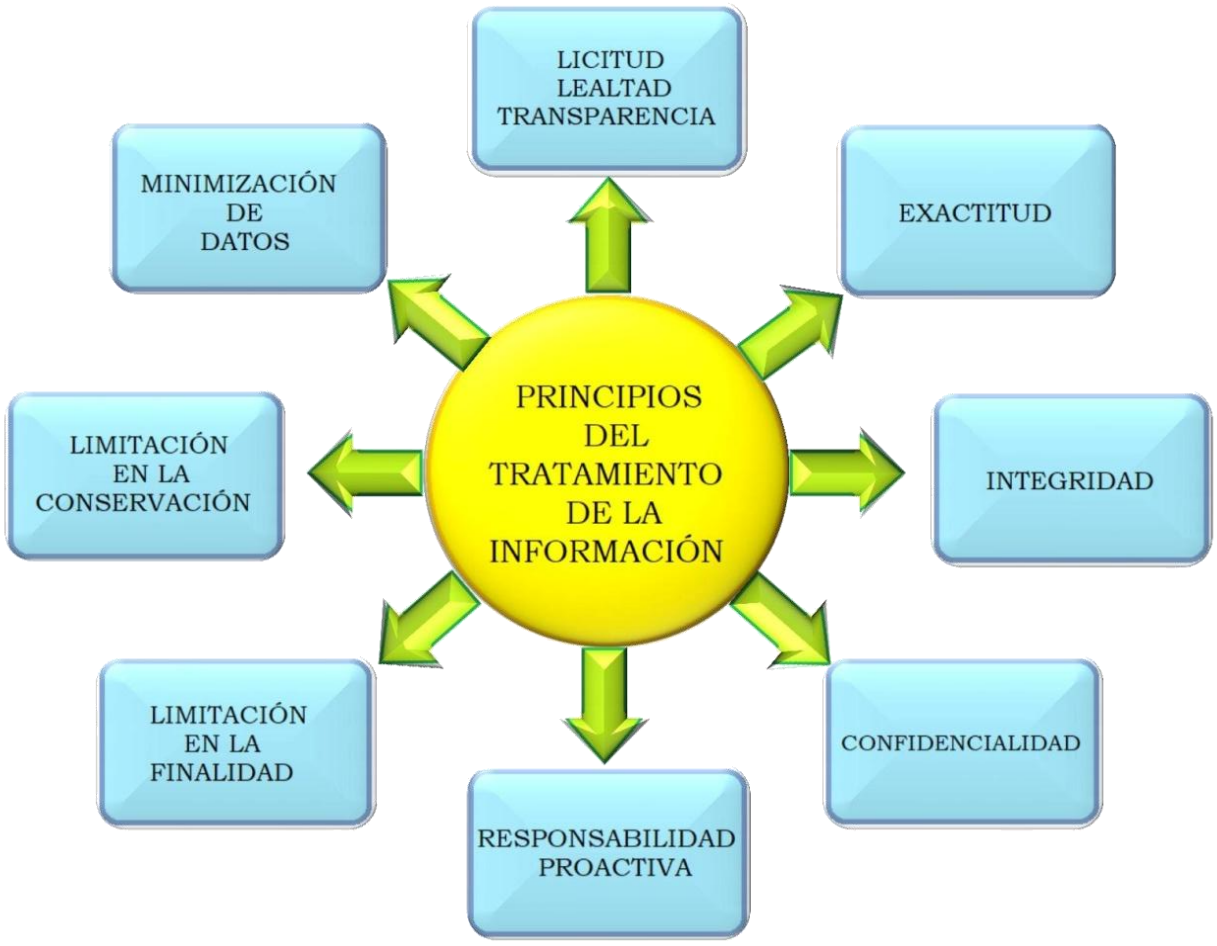
riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión.

- Organización internacional: una organización internacional y sus entes subordinados en Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.
- Representante: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento, represente al responsable o al encargo en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento.
- Responsable del tratamiento o RESPONSABLE: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.
- Servicio de la sociedad de la información: todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, es decir, todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios.
- Seudonimización: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.
- Tercero/a: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.
- Tratamiento transfronterizo:
    - el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o
    - el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro.
- Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimiento automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.
- Violación de la seguridad de los datos personales: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

PRINCIPIOS DE PROTECCIÓN DE DATOS E INFORMACIÓN

1.- Principios fundamentales

- **LICITUD, LEALTAD Y TRANSPARENCIA**. Los datos son tratados de manera lícita, leal y transparente en relación con el interesado.
- **LIMITACIÓN DE LA FINALIDAD**. Los datos son recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.
- **MINIMIZACIÓN DE LOS DATOS**. Los datos serán los adecuados, pertinentes y limitados a lo necesario en relación a los fines para los que son tratados.
- **EXACTITUD**. Los datos serán exactos y, si fuera necesario, serán actualizados. La entidad ha adoptado todas las medidas razonables para suprimir o rectificar sin dilación los datos personales inexactos con respecto a los fines para los que son tratados.
- **LIMITACIÓN DEL PLAZO DE CONSERVACIÓN**. La entidad mantendrá los datos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de dichos datos.
- **INTEGRIDAD Y CONFIDENCIALIDAD**. Los datos son tratados por la entidad de tal manera que se garantiza una seguridad adecuada de los mismos, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de las medidas técnicas y organizativas apropiadas.



ÍNDICE

2.- Principios relativos al tratamiento

La **ENTIDAD** solamente llevara a cabo el tratamiento de datos personales en cumplimiento, **al menos, una de las siguientes condiciones**, en base a su objeto social:
• Consentimiento.
• Relación contractual.
• Interés vital de interesado/a o de otras personas.
• Obligación legal para el/la responsable.
• Interés público o ejercicio de poderes públicos.
• Intereses legítimos prevalentes de responsable o de terceros/as a los que se comunican los datos.

Por este motivo, la **ENTIDAD** identificará claramente la base legal sobre la que se desarrolla el tratamiento, siendo las principales:
- **Consentimiento inequívoco de afectados/as, prestado mediante una manifestación clara afirmativa.**
- **Relación contractual** *(personal laboral y colaboradores*)
- **Obligación legal** (*responsabilidades emanadas de cumplimiento normativo y legal*)

El consentimiento debe ser "inequívoco", definido como aquel que se ha prestado mediante una manifestación de interesado/a o mediante una clara acción afirmativa. No se admiten formas de consentimiento tácito o por omisión, ya que se basan en la inacción.
El consentimiento será, además, "explícito", en las siguientes situaciones:
• **Tratamiento de datos sensibles (**salud, genéticos**), incluidos datos de menores.**
• Adopción de decisiones automatizadas.
• **Transferencias internacionales**.

2.1. Sólo se podrán recabar, usar y conservar los datos de interesado/a que sean adecuados, pertinentes y no excesivos para el fin o el ejercicio de las competencias correspondientes. Queda prohibido el tratamiento de datos por medios fraudulentos, desleales o ilícitos.

El tratamiento de datos que no haya observado los protocolos del sistema de protección de datos de la Entidad se considerará un tratamiento desleal, fraudulento o ilícito, y podrá ser objeto de corrección disciplinaria/administrativa o penal según su gravedad.

2.2. Los datos de carácter personal, por regla general, serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. Los datos personales en posesión de la Entidad no serán conservados en forma que permita la identificación de interesado/a durante un período superior al necesario para los fines para los cuales hubieran sido recabados o registrados, salvo que, y en los términos que establezca la legislación aplicable, resulte necesaria su conservación con el fin de justificar responsabilidades administrativas, laborales y fiscales.

2.3. La forma de conservación de los datos deberá permitir el ejercicio de los derechos de interesado/a. Las normas que regulen el Sistema de Archivos tendrán en cuenta las medidas de seguridad derivadas de la normativa de protección de datos, y prescribirán las medidas necesarias para facilitar el ejercicio de los derechos de los interesados, en especial los de acceso, rectificación y cancelación de los datos, así como cuantos disponga la legislación vigente.

2.4. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades distintas de aquéllas para las que los datos hubieran sido recogidos.

2.5. Los datos personales tratados por la **ENTIDAD** deberán ser exactos y puestos al día de forma que respondan con veracidad a la situación actual de afectado/a. Para que así sea, en los protocolos de recogida de datos se le recordará a interesado/a el deber de que sus datos sean exactos y veraces, y de comunicar a la Entidad cualquier cambio en ellos. La **ENTIDAD** adoptará las medidas pertinentes para garantizar la exactitud y veracidad de los datos y, en su caso, proceder a su corrección. Todo ello

sin perjuicio del derecho de interesado/a, conforme a la legislación vigente, a rectificar los datos que de su persona posea la **ENTIDAD**.

2.6. La **ENTIDAD** informará siempre y en todo caso a interesado/a de modo expreso, preciso e inequívoco del tratamiento al que se sometan sus datos en los términos de RGLMEU y LOPDGDD.

3. Proactividad. Plan de formación

Para la aplicación de las medidas técnicas y organizativas, la **ENTIDAD**, como responsable del tratamiento deberá aplicar las oportunas políticas de protección de datos (apdo. 2, art. 24 RGPD). Se trata de que, en virtud del principio de responsabilidad proactiva (accountability) el/la responsable del tratamiento establezca, cumpla y pueda demostrar, el tratamiento de la información conforme con los principios y medidas de seguridad exigidas en la salvaguarda del derecho a la protección de datos de carácter personal.

Además, el/la responsable del tratamiento tiene que asegurarse de que se cumpla con los requisitos exigibles en virtud de la normativa aplicable a lo largo de todo el ciclo de vida de los datos personales y de la cadena de contratación para dicho tratamiento. Para ello, la **ENTIDAD** facilitará la formación continua en materia de protección de datos, los mecanismos de control periódicos del rendimiento del Sistema de Protección de Datos de la **ENTIDAD** y ordenarán la realización anual de una Evaluación de su Seguimiento, todo ello con el **asesoramiento de DPD**.

CREACIÓN, MODIFICACIÓN, SUPRESIÓN Y GESTIÓN DE INFORMACIÓN

1. Principios generales

1.1. La creación, modificación o supresión de los datos y ficheros de la **ENTIDAD** sólo podrá hacerse mediante dirección u orden del, o de la, responsable designado/a según sus competencias por la **ENTIDAD**, y con el asesoramiento del DPD.

1.2. la **ENTIDAD** confeccionará y mantendrá actualizado un Registro de Actividades, que tendrá a disposición de cualquier interesado/A, debiendo ser publicado en su contenido fundamental en la web corporativa

2. Creación o modificación de ficheros

2.1. En base al objeto social de la **ENTIDAD** y su operatividad, los/las responsables de los distintos departamentos, grupos de estudio/investigación designados/as crearán o modificarán los ficheros de datos, siempre de acuerdo con finalidades lícitas, propias y declaradas.

2.2. Las propuestas deberán contener una memoria justificativa de la creación o modificación del fichero y la información requerida.

2.3. Las disposiciones de creación o de modificación de ficheros deberán indicar:

- La finalidad del tratamiento y los usos previstos para el mismo.
- Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
- El procedimiento de recogida de los datos de carácter personal.
- La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
- Las cesiones de datos y, en su caso, las transferencias de dato que se prevean a países terceros.
- Los/las Responsables del Tratamiento.
- Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición, etc.
- Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

2.4. Ficheros temporales o parciales

2.4.1. Mediante autorización de Responsable del Tratamiento, y con asesoramiento de Responsable de Seguridad/DPD, se podrán crear ficheros temporales o parciales a partir de los ficheros permanentes existentes en la **ENTIDAD**. Dicha autorización deberá contener la identificación de su fichero-fuente, la descripción del contenido de este fichero parcial o temporal, su uso y fin, las personas que tendrán acceso al mismo, su nivel de seguridad y, si fuese el caso, su plazo temporal de uso, así como la indicación del protocolo para su supresión.

2.4.2. Los ficheros temporales se sujetarán a las mismas condiciones de uso y medidas de seguridad que aquél del que se obtuvieron los datos.

2.4.3. Transcurrido el tiempo imprescindible para alcanzar el fin perseguido con los ficheros parciales, se procederá a su supresión.

3. Supresión de bases de datos

Mediante disposición/encargo o supervisado del responsable de la **ENTIDAD**, se acordará la supresión de los ficheros/datos. La supresión de un fichero implica también la de los temporales creados a partir de los datos que en él se contuviesen. En la disposición de supresión se establecerá, el motivo de la misma y el destino de los datos personales contenido en el fichero que será suprimido o, en su caso, las previsiones que se adopten para su destrucción.

ÍNDICE

Si la supresión corresponde al ejercicio de derechos, se actuará conforme a lo establecido normativamente en cuanto a comunicación y transparencia con los usuarios/as.

4. Protocolo de recogida de datos y cláusulas de protección de datos

4.1. La dirección de la **ENTIDAD**, junto al responsable de seguridad y el DPD, supervisarán los protocolos, formularios y procedimientos de recogida de datos personales que sean empleados.

4.2. En todos los protocolos, formularios y procedimientos de recogida de datos se introducirán cláusulas de protección de datos en las que al interesado/a se le informe de:

a. La identidad y los datos de contacto de RESPONSABLE y, en su caso, de su representante;
b. Los datos de contacto del DPD, en su caso;
c. Los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
d. Los destinatarios/as o las categorías de destinatarios de los datos personales, en su caso;
e. En su caso, la intención de responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión.
f. El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
g. La existencia del derecho a solicitar al/la responsable del tratamiento el acceso a los datos personales relativos al/la interesado/a, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
h. La posibilidad de ejercitar todos los derechos que la legislación determine, incluido el derecho a presentar una reclamación ante una autoridad de control;
i. Si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el/la interesado/a está obligado/a a facilitar los datos personales y está informado/a de las posibles consecuencias de que no facilitar tales datos;
j. La existencia de decisiones automatizas, incluida la elaboración de perfiles, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el/la interesado/a.

4.2.1. Cuando la **ENTIDAD** responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al/la interesado/a, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente. De no constar disposición legal que presente excepciones

4.2.2. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el/la interesado/a ya disponga de la información.

4.3. Las cláusulas de protección de datos deben ubicarse en lugar bien visible, de forma perfectamente identificable y legible, anexándose de forma clara e identificable, al resto de trámites del expediente o actuación que se siga en la que resulte necesario recabar datos, y de los formularios empleados por la **ENTIDAD** para la recogida de datos. En el caso de formularios electrónicos, éstos sólo se desbloquearán una vez se cubra la casilla en la que el/la interesado/a declara haber leído la cláusula de protección de datos.

El personal al servicio de la **ENTIDAD** que atienda a los interesados de forma verbal velará de forma diligente porque éstos reparen en las cláusulas de protección de datos pertinentes y atiendan a lo establecido en ellas, recogiendo en las formas previstas por la Entidad el consentimiento.

4.4. En las cláusulas de protección de datos se informará al/la interesado/a de su deber de revelar datos exactos y veraces, y del ejercicio de sus derechos en base a lo determinado por el RGLMEU y la LOPDyGDD.

4.5. Cuando los datos de carácter personal no hayan sido recabados del, de la, interesado/a, este/a deberá ser informado/a de forma expresa, precisa e inequívoca, por la **ENTIDAD**, dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes. Se le facilitará toda la información exigida en la recogida de datos, así como la fuente de su obtención y si está previsto comunicarlos a otro destinatario/a, además de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, y de la identidad y dirección del responsable del tratamiento.

4.6. En el caso de que los datos personales se hayan obtenido de fuentes accesibles al público o de una actividad publicitaria o prospección comercial se informará a interesado/a en los mismos términos.
4.7. En el caso de que la recogida de datos se haga de forma telefónica, por videoconferencia, internet o por cualquier otro modo telemático de comunicación, se le leerá a interesado/a la cláusula de protección de datos que corresponda. Esta lectura será preferentemente grabada, así como la declaración del, de la, interesado/a de que ha sido informado/a sobre el tratamiento de sus datos personales. Al, a la, interesado/a se le informará previamente de que esta parte de su comunicación será grabada y conservada en el expediente que oportunamente se forme con ocasión de su comunicación.

5. Prestación del consentimiento

5.1. Para la recogida y el tratamiento de los datos personales es necesario recabar el consentimiento del, de la, interesado/a, que podrá ser expresado de forma escrita/ digital o verbal, siempre conservando justificante del mismo. Se señala especialmente que la recogida y tratamiento de datos de **MENORES** exige un control especial del consentimiento y conformidad de representación legal, sobre todo en menores de 14 años.
5.2. En ningún caso se cederán datos a terceros, sin el previo consentimiento expreso del, de la, interesado/a, salvo que ese tercero/a sea el/la representante legal del, de la, interesado/a, se haya obtenido consentimiento para la cesión, o sea exigible por disposición legal o necesaria para el cumplimiento de las finalidades declaradas, extremo este del cual se habrá informado.
5.3. Deberá informarse con claridad al, a la, interesado/a de la finalidad a que se destinarán los datos. En caso de comunicación a tercero, también se informará sobre la finalidad del cesionario/a o el tipo de actividad de aquel/aquella a quien se pretenden comunicar.
5.4. Las cláusulas de protección de datos en las que el/la interesado/a haya declarado estar informado/a, o haya consentido, en su caso, el tratamiento de sus datos, se conservarán en los expedientes en los que se haya hecho uso, sin que puedan ser separadas del expediente o almacenadas en lugar distinto o sometidas a un régimen de conservación y archivo distinto.
5.5. En caso de fallecimiento del, de la, interesado/a, y si resultase necesario obtener su consentimiento para el uso y cesión de sus datos, éste deberá recabarse de sus herederos si los hubiere. De no existir o ser imposible su localización, los datos no serán cedidos a terceros salvo que así lo imponga una norma con rango de ley.

6. Revocación, bloqueo y cancelación

El/la interesado/a podrá revocar su consentimiento u oponerse al tratamiento de datos en los términos previstos en la normativa vigente. La revocación deberá hacerse de forma expresa y provocará el bloqueo de los datos. En el caso de que la revocación del consentimiento suponga la imposibilidad de seguir la relación de servicios/contractual, se informará al, a la, interesado/a de esta circunstancia y de que el expediente será archivado y cancelados sus datos personales. No obstante, se le informará de que algunos datos hechos públicos en las actividades de la **ENTIDAD** pueden estar fuera de su responsabilidad, así como de la no retroactividad en los archivos de actividades e histórico de la **ENTIDAD.**

7. Datos especialmente protegidos y los datos relativos a la salud

7.1. Sólo podrán recogerse y tratarse datos relativos a ideología, afiliación sindical, religión y creencias, origen racial o étnico, a la salud y a la vida sexual cuando sea estrictamente necesario para el ejercicio de las competencias/finalidades de la **ENTIDAD** (se reseña la recogida de información sindical y de condiciones de salud o económicas para la contraprestaciones laborales y económicas), y recabando el consentimiento expreso y por escrito del, de la, interesado/a, a quien se le informará de su derecho a no declarar sobre los datos relativos a la ideología, religión, creencias o afiliación sindical o política.
7.2. La **ENTIDAD** sólo podrán usar datos relativos a la ideología, creencias, filiación sindical, salud, origen racial o étnico, y vida sexual, si:

- ✓ El/la interesado/a dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados;

- ✓ El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social;
- ✓ El tratamiento es necesario para proteger intereses vitales del/la interesado/a o de otra persona física, en el supuesto de que el interesado/a no esté capacitado, física o jurídicamente, para dar su consentimiento;
- ✓ El tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;
- ✓ El tratamiento es necesario por razones de un interés público esencial, debiendo ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del/la interesado/a;
- ✓ El tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, o en virtud de un contrato con un/a profesional sanitario y sin perjuicio de las condiciones y garantías exigidas;
- ✓ El tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, con las medidas adecuadas y específicas para proteger los derechos y libertades del/la interesado/a, en particular el secreto profesional,
- ✓ El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, lo que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del/la interesado/a.

7.3. Queda prohibida cualquier cesión de datos sensibles o relativos a la salud del, de la, interesado/a, a terceros, privados o públicos, que no lo sea en el ejercicio de las competencias legalmente atribuidas a la **ENTIDAD** y consentimiento prestado**.**

8. Protocolo de bloqueo, cancelación y destrucción de datos personales

El Protocolo de Seguridad establecerá los procedimientos para el bloqueo, cancelación y destrucción de los datos personales en posesión de la **ENTIDAD** de acuerdo con lo señalado en la normativa aplicable en materia de archivos. El bloqueo y cancelación supondrán la imposibilidad de cualquier comunicación y acceso no autorizado. Esto no supone su destrucción, si no solo su no disposición para cualquier tratamiento no exigido legalmente. Los datos no podrán ser destruidos mientras subsista cualquier responsabilidad administrativa, laboral o fiscal (estimadas en estos ámbitos en unos 5 años, los datos de investigación biomédica pueden tener un plazo de 25 años).

CESIONES, COMUNICACIÓN Y TRATAMIENTO POR CUENTA DE TERCEROS

1. Criterio general. La **ENTIDAD** sólo cederá datos personales obrantes en su poder a terceros en el cumplimiento de una obligación legal de hacerlo o cuando resulte necesario para el ejercicio de sus propias competencias y siempre ateniéndose a lo establecido en la disposición creadora del fichero. Se comprobará la seguridad y cumplimiento legal del "receptor", así como la licitud de las transferencias, sobre todo en el caso de ser de carácter internacional.

1.1. Si bien la LOPDGDD señala en su art. 33:
Artículo 33. Encargado del tratamiento.
1. El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente ley orgánica y en sus normas de desarrollo.

Hay que comprender la diferencia conceptual de términos como "cesión" y "comunicación", el primero otorga potestad sobre los datos, mientras que el segundo solo y exclusivamente informa sobre los mismos. A modo de ejemplo, en el asesoramiento laboral se reciben los datos de trabajadores/as bajo la finalidad de realizar las nóminas, en este caso se trata de un Encargado de Tratamiento al cual se le comunican los datos para una finalidad, no se "ceden", o bien en la disposición pública de listados de opositores/as, donde claramente no se faculta para ninguna finalidad distinta a la mera información. Por otro lado, los casos de cesión establecen generalmente una relación de corresponsabilidad o responsabilidad, en este sentido, en nuestro ámbito, se contemplarían las cesiones de datos entre la UMA y FIMABIS o el SAS, en la cual cada entidad adquiere el derecho de tratamiento para determinados fines propios.

1.2. En el caso de que los datos se comuniquen/cedan entre entidades vinculadas organizativamente, pero siendo entidades con personalidad jurídica propia, con la **ENTIDAD** se deberá informar al/la interesado/a en la recogida y al recabar su consentimiento.

2. Cesión de datos a terceros

2.1. Sólo será posible la cesión a terceros de datos personales, si entra dentro de las condiciones de licitud y si previamente se ha informado al/la interesado/a de esta posible cesión y sus fines, y siempre que se haya obtenido su consentimiento.

2.2. No será necesario ese consentimiento previo si la cesión tiene lugar en el cumplimiento de una obligación legal, o si la cesión es a otra Entidad vinculada para ejercer competencias/finalidades vinculadas al objeto inicial de su recogida. En estas cesiones, se incorporará una cláusula que advierta al cesionario/a del deber de confidencialidad sobre dichos datos. Tampoco requerirá el consentimiento previo del, de la, interesado/a la cesión de sus datos a jueces, tribunales, a defensor del Pueblo o instituciones autonómicas similares, y al Tribunal de Cuentas o instituciones autonómicas similares.

2.3. Podrán cederse datos a terceros, públicos o privados, sin previo consentimiento de interesado/a si se destinan a fines estadísticos, científicos o históricos previa su disociación/seudonimización.

2.4. Por regla general no se incorporarán datos personales a las comunicaciones externas que no lo requieran para surtir sus efectos. En caso de duda, se consultará a Responsable o DPD.

ÍNDICE

2.5. La **ENTIDAD** mantendrá en el Registro de Actividades, un control de cesiones de datos a terceros en el que se inscribirá la identidad y dirección del cesionario/a, fecha de la cesión, fines de la cesión, si es o no conocida por el/la interesado/a, si la cesión ha sido o no consentida, y cualquier otra circunstancia que resulte conveniente.

3. Comunicación de datos de terceros a la ENTIDAD

En el ejercicio de sus competencias, si la **ENTIDAD** debiera acceder a datos de terceros no obtenidos directamente de interesado/a, deberá hacerlo respetando las reglas previstas en este Código y conforme a la legislación aplicable en la materia, informando al/la interesado/a de todos los extremos exigibles.

4. Transferencia internacional de datos

Las comunicaciones de datos a terceros ubicados en otros Estados se realizarán atendiendo a lo dispuesto en la normativa vigente. Teniendo en cuenta el Espacio Europeo, países de confianza según la AGPD y protocolos/contratos vinculantes. El Responsable, asesorado por DPD, autorizará los trámites necesarios para los movimientos internacionales de datos personales.

5. Tratamiento de datos por cuenta de Terceros

5.1. La **ENTIDAD**, con el asesoramiento de DPD, podrá autorizar, el encargo a terceros de tratamiento de datos personales para el cumplimiento de alguna de sus funciones (laboral, fiscal, informática, mensajería, vigilancia etc.). La **ENTIDAD** actuará de forma diligente al elegir a un encargado del tratamiento, siendo, en todo caso, aquel/aquella que ofrezca garantías suficientes respecto a la implantación y el mantenimiento de las medidas técnicas y organizativas apropiadas conforme a lo establecido por el RGLMEU y LOPDGDD, y que garantice la protección de los derechos de las personas afectadas.

5.2. Los tratamientos de datos por cuenta de la **ENTIDAD** se sujetarán a lo dispuesto en la normativa vigente, de seguridad, confidencialidad y responsabilidad.

5.3. El tratamiento de datos por un Encargado de tratamiento no se considerará cesión de datos

La **ENTIDAD** dispondrá de los formatos exigibles para los contratos de Encargado de Tratamiento/mantenimiento/Corresponsabilidad

RGLMEU art. 28: 3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

- *Tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;*
- *Garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;*
- *Tomará todas las medidas necesarias de conformidad con el artículo 32;*
- *Respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;*
- *Asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el cap. III;*
- *Ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;*
- *A elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;*
- *Pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.*

JUSTIFICACIÓN SEGURIDAD Y CONFIDENCIALIDAD

1. Protocolo de Seguridad.

La **ENTIDAD**, asesorada por DPD, el/la Responsable de Seguridad y Responsable de Seguridad de Servicios Informáticos, ordenará la adopción por los/las responsables de los distintos departamentos/comisiones/funciones de las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

Dichas medidas se recogerán en un Protocolo de Seguridad del Registro de Actividades, que será aprobado por la **ENTIDAD**

2. Alcance del Protocolo.

No se registrarán, ni se tratarán, datos de carácter personal e información en ficheros que no reúnan las condiciones de seguridad previstos en el Protocolo de Seguridad.

3. Secreto.

Todo el personal de la **ENTIDAD** y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal e información, pertenezcan o no a la misma, están obligados/as al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con la **ENTIDAD**.

4. Incidencias.

El procedimiento de notificación y gestión de incidencias contendrá necesariamente un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma.

5. Notificación de una violación de la seguridad.

En caso de violación o de la seguridad de los datos, o sospecha de la misma, se notificará al/la responsable de Seguridad, Responsable de Seguridad informática y DPD. De darse tal circunstancia, la **ENTIDAD** notificará a la autoridad de control competente a más tardar en 72 horas desde que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si dicha notificación no se produce en ese plazo de 72 horas, se indicarán los motivos de la dilación.

Contenido mínimo de la comunicación:

- Descripción de la naturaleza de la violación de la seguridad de los datos personales, indicando si es posible, las categorías y el número aproximado de interesados y registros de datos personales afectados;
- Nombre y datos de contacto de DPD o de otro punto de contacto en que se pueda obtener más información;
- Descripción de las posibles consecuencias de la violación de la seguridad de los datos;
- Descripción de las medidas adoptadas o propuestas por la entidad para remediar dicha violación, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos provocados por la misma.

La **ENTIDAD** documentará cualquier violación de la seguridad de los datos personales, relatando los hechos relacionados con la misma, así como sus efectos y las medidas correctivas adoptadas, quedando dicha documentación a disposición de la autoridad de control competente.

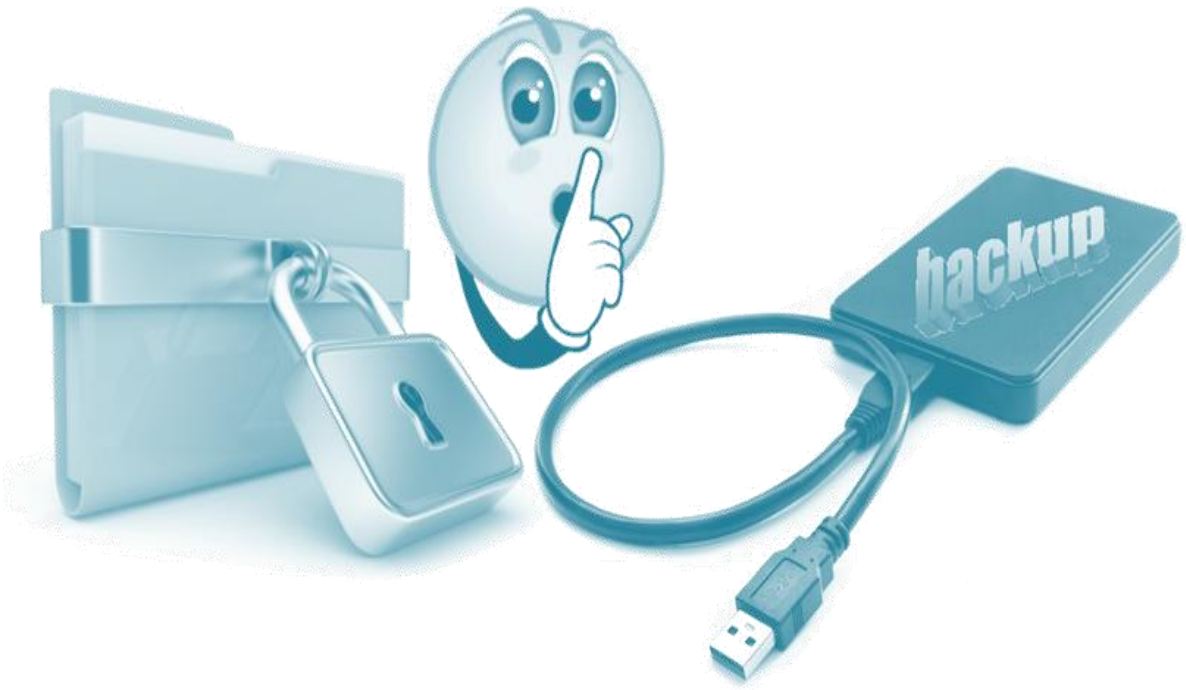
En el supuesto de que la violación de la seguridad de los datos pueda entrañar un alto riesgo para los derechos y libertades de las personas físicas, la **ENTIDAD** la comunicarán a los/las interesados/as afectados/as. Dicha comunicación describirá de forma clara y sencilla la naturaleza de la violación de la seguridad producida y contendrá, como mínimo:

- Nombre y datos de contacto de DPD o de otro punto de contacto en que se pueda obtener más información;

- Descripción de las posibles consecuencias de la violación de la seguridad de los datos;
- Descripción de las medidas adoptadas o propuestas por la entidad para remediar dicha violación, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos provocados por la misma.

La comunicación al/la interesado/a no será necesaria si se cumple algunas de las siguientes condiciones:

- la **ENTIDAD** ha aplicado medidas de protección técnicas y organizativas apropiadas a los datos personales afectados por la violación de la seguridad de los datos personales, especialmente aquellas que hagan ininteligibles los datos personales para cualquier persona no autorizada a acceder a ellos;
- la **ENTIDAD** ha adoptado medidas ulteriores que garantizan que ya no existe la probabilidad de que se concretice un alto riesgo para los derechos y libertades del/de la interesado/a;
- La comunicación supone un esfuerzo desproporcionado para la **ENTIDAD**, pudiendo optarse por una comunicación pública o similar para informar a los/las interesados/as.



CAPTACIÓN Y TRATAMIENTO DE IMÁGENES

A.- CÁMARAS Y FINALIDAD DE SEGURIDAD Y CONTROL LABORAL (VIDEOVIGILANCIA)

1. UBICACIÓN DE LAS CÁMARAS: Se evitará la captación de imágenes en zonas destinadas al descanso de los/las trabajadores/as.
2. UBICACIÓN DE MONITORES: Los monitores donde se visualicen las imágenes de las cámaras se ubicarán en un espacio de acceso restringido de forma que no sean accesibles a terceros.
3. CONSERVACIÓN DE IMÁGENES: Las imágenes se almacenarán durante el plazo máximo de un mes, con excepción de las imágenes que sean aportadas a los tribunales y las fuerzas y cuerpos de seguridad.
4. DEBER DE INFORMACIÓN: Se informará acerca de la existencia de las cámaras y grabación de imágenes mediante un distintivo informativo donde mediante un pictograma y un texto se detalle el responsable ante el cual los/las interesados/as podrán ejercer su derecho de acceso. En el propio pictograma se podrá incluir el texto informativo. En la página web de la Agencia disponen de modelos, tanto del pictograma como del texto.
5. CONTROL LABORAL: Cuando las cámaras vayan a ser utilizadas con la finalidad de control laboral según lo previsto en el artículo 20.3 del Estatuto de los Trabajadores, se informará al/la trabajador/a o a sus representantes acerca de las medidas de control establecidas por la ENTIDAD con indicación expresa de la finalidad de control laboral de las imágenes captadas por las cámaras.
6. DERECHO DE ACCESO A LAS IMÁGENES: Para dar cumplimiento al derecho de acceso de los/las interesados/as se solicitará una fotografía reciente y el DNI del/de la interesado/a, así como el detalle de la fecha y hora a la que se refiere el derecho de acceso.
7. No se facilitará al/la interesado/a acceso directo a las imágenes de las cámaras en las que se muestren imágenes de terceros. En caso de no ser posible la visualización de las imágenes por el/la interesado/a sin mostrar imágenes de terceros, se facilitará un documento al/la interesado/a en el que se confirme o niegue la existencia de imágenes del/de la interesado/a.

B.- CAPTACIÓN Y GRABACIÓN ACTOS PÚBLICOS

En base a la propia caracterización de la **ENTIDAD**, esta puede desarrollar actos públicos en los cuales la participación es voluntaria y la captación de imágenes es notoriamente manifiesta, lo cual no obliga a medidas especiales, salvo el caso de tratamiento de datos que puedan estar protegidos por derechos de propiedad intelectual, ante lo cual se requerirá consentimiento expreso.

En base a la globalización de la tecnología y la comunicación, es recomendable que las personas conozcan las repercusiones que la difusión de imágenes en medios de comunicación y redes sociales con lleva.

ÍNDICE

MEDIDAS DE RESPONSABILIDAD ACTIVA

1. Seguridad del tratamiento (art. 32 RGLMEU). Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el/la responsable y el/la encargado/a del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

- la seudonimización y el cifrado de datos personales;
- la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
- la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
- un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Registro de Actividades de Tratamiento. La **ENTIDAD** redactará y desarrollará un Registro de Actividades

Dicho registro contendrá la siguiente información:

- Nombre y datos de contacto del/de la responsable y, en su caso, del/de la corresponsable, de representantes, si lo hubiese, y de DPD, si existiese.
- Finalidad del tratamiento.
- Descripción de las categorías de interesados/as y de las categorías de datos personales.
- Categorías de destinatarios/as a quienes se han comunicado o comunicarán los datos personales.
- En su caso, las transferencias de datos personales a un tercer país o a una organización internacional y, en su caso, la documentación de las garantías adecuadas adoptadas para la protección de dichos datos.
- Cuando sea posible, plazos previstos para supresión de las diferentes categorías de datos.
- Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad aplicadas

En los casos en que la entidad actúe como encargado/a del tratamiento, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contendrá:

- Nombre y datos de contacto del encargado/a y de cada responsable por cuenta del cual actúa la entidad y, en su caso, de representantes, y del DPD, si existiese;
- Categorías de tratamientos efectuados por cuenta de cada responsable;
- En su caso, las transferencias de datos personales a un tercer país u organización internacional y, en su caso, la documentación de las garantías adecuadas adoptadas para la protección de los datos personales;

3. Análisis de Riesgo. La **ENTIDAD** llevará a cabo una valoración del riesgo con carácter previo a todo nuevo tratamiento con el fin de establecer las medidas de seguridad adecuadas para garantizar los derechos y libertades de los/las interesados/as afectados/as por dicho tratamiento. Este análisis de riesgo variará en función del:

- Los tipos de tratamiento.
- La naturaleza de los datos.
- El número de interesados/as afectados/as.
- La cantidad y variedad de tratamientos llevados a cabo.

Para un adecuado diseño de las actividades de tratamiento de la **ENTIDAD**, se tendrá en cuenta las siguientes consideraciones:

Gestión de riesgos:

- Identificar amenazas y riesgos, entendiendo por amenaza cualquier riesgo con potencial para provocar un daño o perjuicio a los/las interesados/as sobre cuyos datos de carácter personal se realiza un tratamiento.
- Evaluar los riesgos, es decir, valorar el impacto de la exposición a la amenaza, junto con la probabilidad de que esta se materialice, determinándose el impacto en base a los posibles daños que se pueden producir si la amenaza se materializa.
- Tratar los riesgos con el objetivo de disminuir su nivel de exposición con medidas de control que permitan reducir la probabilidad y/o impacto de que estos se materialicen.

Los principales riesgos para los derechos y libertades de las personas físicas se pueden diferenciar en dos dimensiones:

- Riesgos asociados a la protección de la información, pudiendo categorizar las amenazas en 3 tipos:
  - Acceso ilegítimo a los datos, es decir, violación de la confidencialidad.
  - Modificación no autorizada de datos, por tanto, se pone en riesgo la integridad de los mismos.
  - Eliminación de los datos, afectando a su disponibilidad.
- Riesgos asociados al cumplimiento de los requisitos regulatorios relacionados con los derechos y libertades de los interesados.

Dada la variabilidad de los riesgos, la **ENTIDAD** dispondrá de una descripción detallada de los tratamientos que lleva a cabo, de su contexto y de los elementos más relevantes que intervienen en los mismos con el fin de revisar el análisis de riesgo ante cualquier variación en dichos tratamientos que pueda derivar en la aparición de nuevos riesgos.

4. Evaluación de Impacto, relativa al tratamiento de la información. La **ENTIDAD** llevará a cabo una evaluación previa del impacto de las operaciones de tratamiento que vaya a iniciar, cuando sea probable que dicho tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas en base a su naturaleza, alcance, contexto o fines, con el objetivo de determinar, en su caso, la viabilidad o no del tratamiento, y las medidas de control más adecuadas para reducir el nivel de riesgo entrañado hasta un nivel considerado aceptable.

La obligación de realizar una evaluación de impacto corresponde a la **ENTIDAD**, con el asesoramiento de DPD, si ha sido nombrado/a.

Se requerirá, especialmente, realizar una evaluación de impacto en caso de:

- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
- Tratamiento a gran escala de categorías especiales de datos o de datos personales relativos a condenas e infracciones penales; o
- Observación sistemática a gran escala de una zona de acceso público.
- Debe considerarse así mismo en entidades con tratamiento de datos de menores

La evaluación deberá contener como mínimo:

- Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento;
- Una evaluación de la necesidad la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
- Una evaluación de los riesgos para los derechos y libertades de los/las interesados/as;
- Las medidas previstas para afrontar los riesgos, incluidas las garantías, medidas de seguridad y mecanismos que garanticen la protección de los datos personales.

Si de la evaluación de impacto llevada a cabo por la **ENTIDAD**, se determina que la operación de tratamiento presenta un riesgo residual, es decir, el riesgo una vez que se han aplicado las medidas de control para mitigar y/o reducir el impacto asociado a dicho riesgo, es alto o muy alto, realizará una consulta a la autoridad de control que deberá incluir:

- Las responsabilidades respectivas de la entidad, corresponsabilidad y encargados/as del tratamiento implicados en el tratamiento, en su caso;
- Las medidas y garantías establecidas para proteger los derechos y libertades de los/las interesados/as;
- Los datos de contacto de DPD, si ha sido nombrado/a;
- Cualquier otra información que solicite la autoridad de control.

En función de la resolución a la que llegue la autoridad de control, establecerá las condiciones y medidas que se deben aplicar para llevar a cabo el tratamiento o, en su caso, que no se podrá llevar a cabo.

5. Delegado/a de Protección de Datos. Designación del delegado/a de protección de datos

(art. 37 RGLMEU) *1.El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que: I.- el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial; II.- las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, III.- las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales*

(Artículo 34 LOPDGDD). *1. Los/las responsables y encargados/as del tratamiento deberán designar un delegado/a de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:*

a. *Los colegios profesionales y sus consejos generales.*
b. *Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.*
c. *Las entidades que exploten redes y presten servicios de comunicaciones electrónicas. Los prestadores de servicios de la sociedad de la información.*
d. *Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito. Los establecimientos financieros de crédito. Las empresas de servicios de inversión. Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude*
e. *Las entidades aseguradoras y reaseguradoras.*
f. *Los distribuidores y comercializadores de energía eléctrica y gas natural.*
g. *Las entidades que desarrollen actividades de publicidad y prospección comercial.*
h. *Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes. Se exceptúan los profesionales de la salud que ejerzan su actividad a título individual.*
i. *Las entidades que tengan como uno de sus objetos la emisión de informes comerciales*
j. *Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.*
k. *Las empresas de seguridad privada.*
l. *Las federaciones deportivas cuando traten datos de menores de edad.*

Funciones de DPD

El delegado/a de protección de datos tendrá como mínimo las siguientes funciones:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

- Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación;
- Cooperar con la autoridad de control; e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento y realizar consultas, en su caso, sobre cualquier otro asunto.
- El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

MEDIDAS BÁSICAS PRÁCTICAS

1. INTRODUCCIÓN. Todo el personal que acceda/trate la información de la **ENTIDAD** está obligado a conocer y observar las medidas, normas, protocolos, reglas y estándares que afecten a las funciones que desarrolla. Cada persona se responsabiliza del puesto de trabajo o funciones que tenga asignadas y debe cumplir con los procedimientos internos de la **ENTIDAD** con respecto a la protección de datos personales.

2. BUENAS PRÁCTICAS GENERALES

Se debe disponer de:

- ✓ **REGISTRO DE ACTIVIDADES,** actualizado y con toda la información exigida en base al ámbito de tratamiento
- ✓ **AUDITORÍAS PERIÓDICAS,** con gestión de registros de incidencias, control de personal y terceros, ejercicio de derechos, sistemas de tratamiento y archivo tanto informático como documental

Control sobre:

- ➢ **GESTIÓN DOCUMENTAL:**
  - Se dispondrá de formatos de recogida de datos correctamente redactados
  - Los datos serán, en la medida de lo posible, y en base a su valor de riesgo, anonimizados o seudonimizados
  - Se dispondrá de Documentos de Responsabilidad para todo usuario/a con acceso a la información
  - Se dispondrá de contratos de Encargados/as de Tratamiento que recojan todas las obligaciones legales
  - Se dispondrá de formatos para el ejercicio de los derechos dispuestos por la legislación vigente
  - Se dispondrá de los preceptivos avisos legales y políticas de privacidad

- En la recogida de información se deberá informar de todos los extremos exigidos por la normativa vigente, debiendo recurrir a los formatos preestablecidos por la **ENTIDAD**, o en todo caso al asesoramiento del DPD. Con especial consideración en el tratamiento de datos de carácter especialmente sensible, como salud, ideología o menores.

- Se deberá **guardar el debido secreto y confidencialidad** sobre la información que conozcan en el desarrollo de su trabajo. Esta obligación de guardar secreto subsistirá aún después de finalizar las relaciones contractuales con la organización. **No sacar información ni datos personales** de la **ENTIDAD** salvo en los casos que lo requieran las funciones asignadas y, en su caso, previa autorización.

- En el tratamiento de la información, ya sea en formato documental o informatizado, se debe preservar la discreción y confidencialidad. Para ello se determinarán los/las responsables de anonimización de aquellos datos que así se requiera (datos de salud), y sistemas de su procesamiento

- Cuando se atiende al público, personal no autorizado, o se abandona el lugar de trabajo, bien temporalmente o bien al finalizar el turno, se debe dejar en un estado que **impida la visualización de los datos protegidos:**
  - **No dejar documentos con datos de carácter personal a la vista**
  - **Bloquear el equipo** con contraseña o desconectándose de las aplicaciones y la red, y **apagando el monitor**.
  - **Inmediatamente comunicar** al/la Responsable de Seguridad y DPD cualquier **solicitud de ejercicio de derecho de acceso, rectificación, cancelación, oposición o cualquier otro que determine la legislación vigente** de los datos por parte de su titular. Existen unos plazos legales ajustados para responder a dichas solicitudes.

- Con respecto a los **ordenadores portátiles y resto de dispositivos de almacenamiento móviles (teléfonos móviles, memorias USB, etc.)**, se debe evitar en la medida de lo posible su uso, no obstante, se debe cumplir:

ÍNDICE

- Mantenerlos siempre con contraseña y controlados, (no dejar en lugares públicos.) para evitar su sustracción.
- Reducir y/o eliminar la información que no vaya a ser utilizada.

- En caso de:
  - **Cualquier alteración de la operatividad de los sistemas.**
  - **Violación de seguridad, o sospecha de ella.**
  - **Pérdida o robo de un dispositivo de almacenamiento móvil (portátil, teléfono, USB, etc.)**

  Se notificará inmediatamente como incidencia de seguridad a Responsable de la Entidad o a DPD.

- Se debe proporcionar la ayuda que se requiera en lo que se refiere a **mantener la calidad de los datos**, lo cual implica controlar:
  - Que la **información** contenida en los ficheros únicamente sea **tratada en relación con las finalidades** para las que se haya obtenido.
  - Que los datos sean **exactos**, estén **actualizados** y sean **cancelados cuando éstos hayan dejado de ser necesarios.**

3. BUENAS PRÁCTICAS CON INFORMACIÓN EN SOPORTE AUTOMATIZADO

Considerar la información como un activo fundamental de la organización cumpliendo las siguientes medidas:

- En caso de detectar **cualquier indicio de problema de seguridad, inmediatamente debe poner el mismo en conocimiento del/de la Responsable de la Entidad o a DPD.** Entre otras, son incidencias frecuentes las pérdidas de contraseñas o la recuperación de datos por borrado accidental.
- **No realizar acciones que puedan poner en peligro la seguridad de la información** (introducción de software ilegal, envío de información a través de correo electrónico sin las suficientes medidas de seguridad, etc.). Se debe respetar la configuración de aplicaciones corporativas (ofimática, antivirus, etc.) de los puestos de trabajo y sólo podrá ser cambiada bajo la autorización de responsable de seguridad o de los/las administradores/as informáticos/as autorizados/as.
- Se debe **cumplir la política de contraseñas establecida**, especialmente la **periodicidad de cambio (al menos una vez cada 6 meses)**, y utilizar contraseñas de al menos ocho caracteres que combinen números, letras (mayúsculas y minúsculas) y caracteres especiales.
- Es muy importante que **no se almacenen ni traten datos de carácter personal en el disco duro sin clasificación (directamente en escritorio, por ejemplo)**. Dichas acciones deberán realizarse en los entornos provistos al efecto (carpetas de los servidores, aplicaciones, etc.) protegidos mediante identificadores de usuario/a con los permisos correspondientes.
- No se permite el acceso a los sistemas de información con un identificador de usuario/a que no sea el propio, así como comunicarlo o cederlo con su contraseña a cualquier otra persona. Las **contraseñas no deberán anotarse o guardarse en lugares visibles** o fácilmente accesibles.
- **Cada usuario/a se responsabiliza de la confidencialidad de sus contraseñas** y, en caso de que sean conocidas fortuita o fraudulentamente por otras personas, debe comunicarlo como incidencia de seguridad, según el procedimiento establecido y proceder a su cambio inmediato.
- Se recomienda reducir al máximo el almacenamiento de información confidencial y eliminarla cuando haya dejado de ser necesaria. En caso de crear **archivos para uso temporal debe asegurarse su eliminación cuando estos hayan dejado de utilizarse**.
- Se recomienda el uso de almacenamiento y tratamiento seguro, en redes seguras, no en discos duros de pc´s individuales, pendrives, etc., que pueden ser susceptibles de acceso no autorizados. No obstante, de ser necesario, la información como mínimo se guardará bajo contraseña propia, distinta a la dispuesta para acceder al dispositivo

Respecto al **correo electrónico e Internet,** se debe prestar atención al envío de datos de carácter personal por medio del correo electrónico, tanto en el cuerpo del mensaje como en anexos y, si se realiza, tratar esos mensajes y anexos como temporales y borrarlos en cuanto dejen de ser

ÍNDICE

necesarios. **El correo electrónico no es un gestor documental**, los ficheros enviados o recibidos deben estar almacenados en los sistemas y carpetas correspondientes protegidos por las credenciales de usuario/a correspondientes.

Además, se deben evitar realizar las siguientes acciones si el usuario tiene asignada una dirección personal corporativa de la Entidad:

- ✓ Que un empleado/a /usuario/a haga uso de cuenta de correo ajena o permitir a un tercero su uso.
- ✓ El envío de mensajes difamatorios, amenazantes o abusivos transmitiendo cualquier mensaje que puede interpretarse como tal.
- ✓ Transmitir material de la **ENTIDAD** a menos que esté adecuadamente protegido y autorizado.
- ✓ Transmitir identificadores, contraseñas, configuraciones de redes locales o direcciones a través de Internet.
- ✓ Abrir correos procedentes de direcciones desconocidas o que no estén relacionados con motivos de trabajo y ofrezcan suficientes garantías, para evitar la entrada de virus, troyanos o código malicioso.
- ✓ Abrir adjuntos a correos o pulsar en enlaces a menos que sea conocido y de confianza el origen del correo y del enlace.
- ✓ Evitar en los puestos de trabajo la descarga de ficheros e instalaciones de ejecutables procedentes de Internet que no ofrezcan las suficientes garantías sobre su origen e integridad y que no hayan sido debidamente autorizadas.
- ✓ No se pondrán utilizar cuentas de correo personales para el envío de información profesional de la **ENTIDAD** excepto en situaciones inevitables (por ejemplo, ante una urgencia y el sistema esté caído.
- ✓ No se podrá utilizar el correo corporativo para finalidades distintas a las corporativas.
- ✓ No realizar reenvío masivo de correos, y si se ha de hacer, utilizar CCO (con copia oculta), cuando se envía a diferentes destinatarios/as con el fin de ocultar la visualización de direcciones de correo.
- ✓ El uso de Internet no deberá interferir en obligaciones o degradar el servicio a otros/as usuarios/as.
- ✓ Los/las usuarios/as no podrán realizar vistas a sitios web que promuevan actividades ilegales.

• **Ficheros temporales**: los ficheros temporales creados extrayendo datos de las aplicaciones corporativas para la ejecución de una determinada tarea o proceso (ejemplo: listados en Word o Excel) no deben mantenerse indefinidamente ni en el ordenador ni en un directorio de red y una vez finalizada dicha tarea o proceso **hay que eliminarlos**.

3.1.- MEDIDAS TÉCNICAS

IDENTIFICACIÓN

- ➢ Si bien no es recomendable, cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador.
- ➢ Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.
- ➢ Se garantizará la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá al menos 8 caracteres, mezcla de números y letras.
- ➢ Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se dispondrá de un usuario y contraseña específicos (identificación inequívoca).
- ➢ Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. Para la gestión de las contraseñas puede consultar la guía de privacidad y seguridad en internet de la Agencia Española de Protección de Datos y el Instituto Nacional de Ciberseguridad. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas del usuario.

ÍNDICE

DEBER DE SALVAGUARDA

A continuación, se exponen las medidas técnicas mínimas para garantizar la salvaguarda de los datos personales:

- ACTUALIZACIÓN DE ORDENADORES Y DISPOSITIVOS: Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la media posible.
- MALWARE: En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.
- CORTAFUEGOS O FIREWALL: Para evitar accesos remotos indebidos a los datos personales se velará para garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.
- CIFRADO DE DATOS: Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.
- COPIA DE SEGURIDAD: Periódicamente se realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el ordenador con los ficheros originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información.

3.2.1 ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIONES

Toda conexión al sistema de información de FIMABIS mediante accesos remotos, en el caso de que se produzcan, requerirá siempre el mismo nivel de seguridad exigido para el acceso en modo local o red de área local. Con carácter general, el sistema de información garantizará que no se permitan accesos no autorizados mediante la identificación y autentificación de los usuarios que accedan al sistema de forma remota, utilizando identificadores y contraseñas de acceso de uso personal e intransferible.

En el caso de que se produzca algún tipo de transferencia de datos calificados de sensibles, dicha comunicación deberá ser anonimizada o bien cifrada mediante certificado u otro cifrado.

3.1.3. IDENTIFICACIÓN Y AUTENTICACIÓN

FIMABIS ha establecido un procedimiento para la identificación y autenticación del/la usuario/a para su acceso a las aplicaciones donde se encuentran los datos personales e información de los ficheros que consiste en la combinación de un código de identificación de usuario y una contraseña. El acceso a los equipos también requiere la introducción de una contraseña para el inicio de la sesión del/la usuario/a.

En el apartado ***"Gestión de contraseñas"*** se describen los procedimientos establecidos en FIMABIS en relación a las contraseñas.

El control de acceso al sistema y/o aplicaciones limitará el número máximo de intentos fallidos de acceso al sistema y a las aplicaciones a un número de tres a cinco intentos. En este caso, se procederá al bloqueo del/la usuario/a que, para volver a acceder al sistema, deberá solicitarlo o esperar 30 minutos, siguiendo el procedimiento establecido en el apartado ***"Gestión de usuarios"***.

3.1.4.- CONTROL DE ACCESO

Los/las usuarios/as sólo tendrán acceso a aquellos datos y recursos que precisen para el desempeño de sus funciones.

FIMABIS, en función de las tareas que prevea que va a desempeñar cada usuario/a, determinará qué aplicaciones, qué información dentro de estas y qué documentación con datos personales e información serán accesibles por los mismos.

En el apartado ***"Relación de usuarios/as del sistema"***, está destinado a recoger la relación de usuarios/as con acceso autorizado a los ficheros, así como los derechos que tienen concedidos. Esta relación se modificará en caso de que se produzcan cambios.

El/la usuario/a deberá tener configurado su puesto de trabajo para que se exija la introducción de una contraseña al intentar volver al sistema, tras un periodo de entre 10 y 15 minutos de inactividad.

3.1.5.- GESTIÓN DE SOPORTES

En FIMABIS se gestionan soportes documentales e informáticos. Los mismos estarán inventariados e identificarán su contenido, por ejemplo, mediante su etiquetado.

En el caso de que se reciba algún soporte, documental o automatizado, con información personal en FIMABIS debe ser registrado por el destinatario en el registro de entrada, donde se indique la siguiente información:

- Tipo de soporte
- Número de soportes del envío
- Fecha y hora
- Identificación del remitente
- Tipo de información.
- Modo de envío.
- Persona que realiza la recepción que debe estar debidamente autorizada.
- Estado del soporte: Pendiente de proceso/ Custodiado / reutilizado / destruido

Con carácter general, los soportes recibidos en FIMABIS una vez procesados, serán borrados completamente.

En los casos en que se deba conservar el soporte con su contenido, se hará constar en el registro de entrada y anotará la siguiente información en la etiqueta:

- Nombre del departamento.
- Fecha de recepción.
- Referencia del contenido.

Para realizar la salida de soportes con datos fuera de las instalaciones de la fundación, se deben cumplir los siguientes requisitos:

- Contar con autorización del Responsable.
- En el caso de que se contengan datos sensibles, la información deberá anonimizarse o cifrarse de forma que se garantice que no podrá ser manipulada ni accesible por ningún medio durante su transporte.

Al igual que en el caso de los soportes recibidos, también se mantendrá un registro de salida de soportes o documentos con datos fuera de la empresa, a través del registro de salida. Debe registrar la siguiente información:

- Tipo de soporte
- Número de soportes del envío
- Fecha y hora
- Identificación del destinatario
- Tipo de información.

- Modo de envío.
- Persona que realiza el envío que debe estar debidamente autorizada

En el apartado ***"Registro de Entrada y Salida de Soportes"*** se presenta un modelo para llevar a cabo el registro de las entradas y salidas anteriormente citadas.

3.1.6.- PROCEDIMIENTO PARA OBTENER LA AUTORIZACIÓN DE SALIDA DE SOPORTES FUERA DE LAS INSTALACIONES DE LA FUNDACIÓN

El Responsable de los ficheros aprobará las salidas de soportes y documentos con datos autorizadas. Las mismas se relacionan en el apartado ***"Salidas de datos autorizadas"***. En el caso de necesitar una autorización, cuyo modelo se especifica en el citado apartado, para algún soporte que no figure en la mencionada relación, deberá seguirse los siguientes pasos:

- Petición: Solicitud por escrito que deberá contar con el visto bueno del Responsable de Seguridad, que deberá decidir la aprobación o denegación de la solicitud.
- Comunicación: El Responsable de Seguridad comunicará al solicitante la decisión.

3.1.7.- REUTILIZACIÓN, DESTRUCCIÓN Y MANTENIMIENTO SOPORTES

Todos los soportes que no sean inventariados, una vez que hayan sido procesados, serán borrados totalmente antes de ser nuevamente utilizados. También deben ser etiquetados de nuevo para responder al contenido actual.

Deben de cumplir las medidas correspondientes al nivel de seguridad aplicable a los datos que contengan y ser almacenados correspondientemente.

Los soportes que deban desecharse, serán totalmente destruidos antes de ser desechados mediante cortadora de cuadrados.

La destrucción de los soportes debe ser total, dejándolo en un estado en el que no se pueda proceder a recuperar la información que contenía y previamente deben haber sido formateados y borrados.

3.1.8.- CONTROL DE ACCESO FÍSICO

El acceso a las instalaciones de FIMABIS donde se encuentran los equipos, sistemas de información y la documentación con datos está limitado a los usuarios autorizados y que se recogen en este documento. En el caso de que sea necesario que cualquier otra persona permanezca en las instalaciones, siempre será acompañada por algún empleado/a de FIMABIS.

Los equipos y la documentación se encontrarán en lugares donde no puedan acceder personas no autorizadas. Para acceder a las instalaciones es necesario tener llave o acudir en horario de atención al público, donde los usuarios serán recibidos por el personal de la fundación.

4. BUENAS PRÁCTICAS PARA TRATAR INFORMACIÓN EN SOPORTE DOCUMENTAL (NO AUTOMATIZADO)

La confidencialidad de la información se consigue también a través del cuidado del entorno de trabajo, evitando que la misma pueda ser de fácil acceso por cualquiera. Para ello se establecen varias actuaciones de obligado cumplimiento:

- **Mesas limpias**: cada usuario/a, cada vez que se ausente de su mesa de trabajo o bien cuando termine su jornada laboral, deberá retirar toda aquella información que pudiera ser de carácter confidencial.
- **Utilización de fotocopiadoras, escáneres e impresoras**: Al utilizar impresoras o fotocopiadoras, debe asegurarse de recoger los originales al finalizar, y de que no quedan documentos con datos sensibles en la bandeja de salida. Si las impresoras son compartidas con otros usuarios/as sin acceso a los datos que están siendo impresos, se deberán retirar los

documentos conforme vayan siendo impresos. De forma análoga, al utilizar los escáneres debe asegurarse de recoger los documentos originales y, si la carpeta de destino se comparte con usuarios sin acceso a esos datos personales, eliminar el archivo cuanto antes de esa carpeta y trasladarlo a otra carpeta con un nivel de seguridad acorde a los datos que contienen.

- **Eliminación de documentos**: utilizar los dispositivos destinados al efecto para desechar el material correspondiente, es decir, depositarla en los contenedores destinados al efecto o en las destructoras de papel. Si se elimina documentación en las papeleras, ésta deberá romperse previamente de forma que la información en ella contenida quede ininteligible.
- **Distribución de la documentación**: adoptar medidas cautelares que eviten accesos no autorizados. Se pueden producir diferentes situaciones en el movimiento de los ficheros en papel:
  - Envíos fuera de la sede: siempre debe salir en sobre cerrado o dispositivo de seguridad similar que evite accesos de terceros, imposibilitando la consulta, copia o reproducción de la misma.
  - Envíos dentro de la sede: para envíos dentro del mismo edificio donde se encuentra el puesto de trabajo, se deben evitar accesos no deseados. - Verificar que las personas a las que se entrega la documentación original o una copia de la misma la han recibido.
- No retirar de las dependencias soportes o ficheros no automatizados **sin la debida autorización**.

Las medidas de seguridad serán revisadas de forma periódica, la revisión podrá realizarse por mecanismos automáticos (software o programas informáticos) o de forma manual.

En la Oficina de Seguridad del Internauta (https://www.osi.es) el Instituto Nacional de Ciberseguridad (www.incibe.es) se dispone información y herramientas informáticas gratuitas que pueden ser útiles para garantizar la seguridad de los datos personales en ordenadores y dispositivos electrónicos.

CONSECUENCIAS DEL INCUMPLIMIENTO

El personal que intervenga en cualquier fase del tratamiento de la información y que incumpla lo descrito en el presente documento, o en su caso en los documentos, normas o procedimientos relacionados con la seguridad y con la protección de datos de carácter personal, deberá saber que podrá ser sometido al régimen sancionador/disciplinario existente en la organización, todo ello sin perjuicio de las posibles consecuencias civiles y penales a las que hubiera lugar en su caso ante un incumplimiento legal.

RESPONSABILIDAD PROAC

ÁMBITO DE IMPLEMENTACIÓN

I.- RESPONSABLE TRATAMIENTO

Fundación para la Investigación de Málaga en Biomedicina y Salud -FIMABIS-
Instituto de Investigación Biomédica de Málaga y Plataforma en Nanomedicina -IBIMA Plataforma BIONAND-
Ins. Reg. Fundaciones Consejería Justicia y Administraciones Públicas Junta de Andalucía nº MA-606
C.I.F.: G29830643
Parque Tecnológico de Andalucía (PTA)Avenida Severo Ochoa, 35, 29590, Málaga.
tlf. 951 440 260- 951 440 263; fimabis@fimabis.org / ibima@ibima.eu

Delegado Protección de Datos: José Montilla Chicano, DPD_ProteccionDatos@ibima.eu

I.2.- Organigrama de coordinación:

- GERENCIA:……..
- Responsable Seguridad y Sistemas:……
- Coordinación: ……

II. TRATAMIENTO DE INFORMACIÓN.

II.1.- TIPOLOGÍA DE DATOS Y COLECTIVOS

En base a su objeto social se determinan como áreas y ámbito de información:

I.- Área Investigación y Formación

I.i.- Gestión proyectos.

a) Tratamiento de datos personales de usuarios/as, necesarios para la investigación biomédica con inclusión de datos identificativos, de salud, e imagen.
Son proporcionados por los servicios clínicos del SAS adscritos a los proyectos de investigación, con consentimiento informado de interesado/a, no se contempla cesión ni comunicación directa, siendo sometidos a procesos de seudonimización efectiva.
b) Tratamiento de datos bajo finalidad de investigación y/o formación

I.ii.- Gestión personal.

a) Tratamiento de datos personales de personal investigador y colaborador, personal vinculado a investigación y formación, con inclusión de datos identificativos, de contacto, y curriculares, con inclusión de imagen.´ñ.- cedidos/comunicados a las distintas entidades vinculadas, SAS, Universidad de Málaga, así como a otras relacionadas con la investigación y/o formación, y aquellas derivadas de obligaciones legales.
b) Tratamiento de datos bajo finalidad de control y gestión de la investigación y/o formación
c) Tratamiento de datos bajo finalidad de gestión de eventos y actividades promocionales, con posible inclusión de datos de personal responsable, y datos personales de participantes. Con cesión a entidades convocantes y empresas aseguradoras.

II.- Área de Gestión Corporativa

Tratamiento de la información necesaria para la gestión y desarrollo de la propia Entidad

1. **Área Administrativa-Económica**: Control y fiscalización interna de la gestión económico-financiera, presupuestaria y tesorería de la entidad, abarcando las funciones contables, tributarias, fiscales y todas las relativas, en general, a la planificación económica.
    - **Ficheros de Gestión Administrativa-Económica**: estructura general de actividades administrativas, contabilidad/facturación, proyectos, proveedores, etc., Reseñándose datos de identificación, domicilio, servicios prestados, datos bancarios de alumnado y

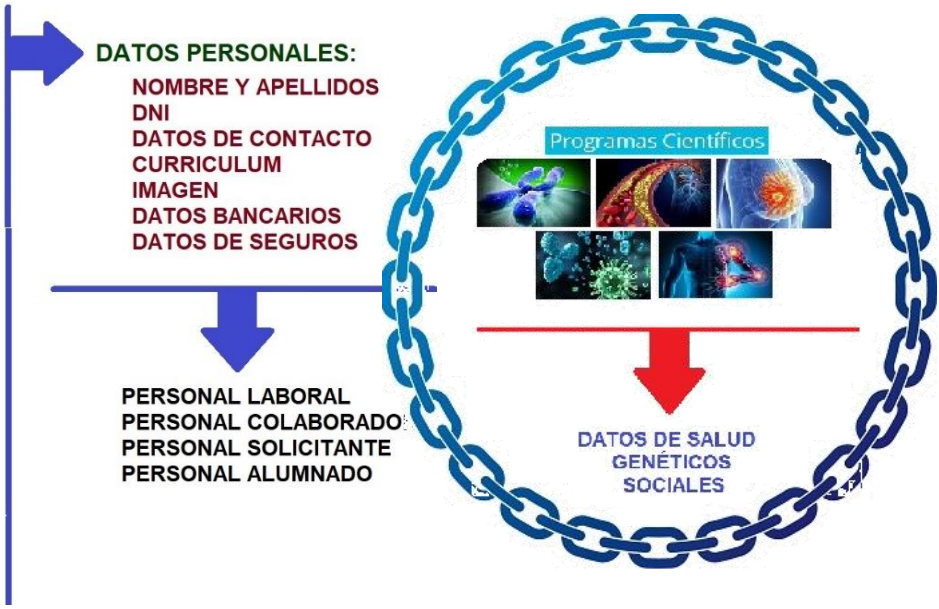
representantes legales. Datos en parte empresariales. Se comunica a la administración compétete tributaria y fiscal.

2. **Área Jurídica**: Estudio, asesoramiento jurídico y propuestas de carácter superior, preparación de los asuntos a estudiar por los órganos resolutivos y actuaciones en materia de gestión laboral e investigadora.
    - **Ficheros generados en el departamento jurídico**, con tratamiento de posibles reclamaciones y cuestiones legales de personal laboral y colaborador vinculado, órganos de dirección y gestión. Acceso restringido a responsable Jurídico, con comunicación a Comisiones competentes, así como administración correspondiente.

3. **Área Recursos Humanos y Organización**: Estudio, informe, gestión, asesoramiento y propuesta en materia de recursos humanos y su formación, así como medidas organizativas de la misma.
    - **Fichero Gestión Laboral y Recursos Humanos**: gestión y tratamiento de los datos de personal, nóminas y curriculum. Servicios de prevención de Riesgos Laborales. Se comunica a la Administración competente, Servicio Empleo, Seguridad Social y otras administraciones con competencia en ámbito laboral, así como aseguradoras.

4. **Área Logística (Técnica y Mantenimiento**): Estudio, informe, asesoramiento y propuesta de carácter técnico, así como la coordinación, dirección y mantenimiento de las instalaciones e infraestructuras.
    - **Fichero vinculado a la gestión Administrativa**

5. **Área de Comunicaciones**: gestión y tratamiento de las comunicaciones y contactos de la Entidad, con seguimiento de registros de entrada y salida, así como la difusión de su ámbito público, todo ello a través de cualquier medio de comunicación. Se incorpora la información a los sectores y áreas pertinentes.
    - **Fichero de Comunicaciones, Agenda de Contactos y Correo Electrónico**: generado y dedicado al control de recursos de comunicaciones y contactos.
    - **Fichero de Gestión WEB**: recoge la información incorporada a través del operativo WEB, incluidas direcciones IP.
    - **Registro de Entrada/Salida** dedicado a la gestión de recepción y envío de documentación oficial.



II.2.- CARACTERIZACIÓN DE LA INFORMACIÓN

COLECTIVOS DATOS	PERSONAL LABORAL	INVESTIGADORES COLABORADORES	SOLICITANTES	ASESORES /PROVEEDORES/ CORRESPONSABLES
Nombre y Apellidos	X	X	X	X (DATOS DE CONTACTO
Razón Social				X
Huella dactilar	X			
Imagen	X	X	X	X
CIF				X
DNI	X	X	X	
Domicilio	X	X	X	X
Telf.	X	X	X	X
Email	X	X	X	X
Videograbación seguridad	X	X	X	X
Datos bancarios	X	X		X
Datos económicos	X	X		
Datos de seguros	X	X		
Currículum académico /laboral	X	X	X	

Específica de ensayos clínicos e investigación

COLECTIVOS DATOS	PERSONAS PARTICULARES-SUJETOS DE ESTUDIO
Nombre y Apellidos	X
Imagen	X
DNI	X
Domicilio	X
Telf.	X
Email	X
Videograbación seguridad	X
DATOS DE SALUD/CREENCIAS	X
Datos Sociales/Laborales	X
Currículum académico /laboral	X

ÍNDICE

II.2.- CARACTERIZACIÓN EN BASE A FINALIDAD.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

1.i- AREA INVESTIGACIÓN Y FORMACIÓN. Gestión Proyectos

a) Base jurídica	RGPD: 6.1 a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física; e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Ley 14/2007, de 3 de julio, de Investigación biomédica Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación Ley 41/2002, de 14 de noviembre, básica reguladora autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Ley 1/2014, de trasparencia pública de Andalucía
b) Fines del tratamiento	Gestión y control de las actividades investigadoras en el ámbito de la biomedicina. Gestión de proyectos y publicaciones
c) Colectivo	Personas voluntarias y pacientes del SAS, bajo consentimiento informado
d) Categorías de Datos	Nombre y apellidos, Nº Registro sanitario, imagen, datos genéticos, datos de salud, datos sociales
e) Categoría destinatarios	Los datos personales identificativos, no serán cedidos, salvedad hecha de obligación legal a las Administraciones competentes sanitarias y organismos y entidades colaboradoras.
f) Transf. Internacional	Los datos personales identificativos, no serán cedidos. No obstante, los datos de investigadores, como profesionales involucrados en los proyectos, podrán ser comunicados a entidades colaboradoras
g) Plazo supresión	Serán seudonimizados/anonimizados de forma fehaciente, no obstante, en base a su carácter vinculado a la salud, y por exigencias legales podrían ser conservados para determinar posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. Será de aplicación lo dispuesto en la normativa de archivos y documentación, y conservación de registros de investigación.
h) Medidas de seguridad	Las medidas de seguridad implantadas se corresponden con las previstas en el Reglamento Europeo 2016/679 de protección datos de carácter personal y L.O.P.D.G.D.D. 3/2018, y ENS Control de accesos y autorizaciones. Seguridad física infraestructuras y edificios Seguridad lógica de sistemas. Seguridad de redes. Compromiso fehaciente de confidencialidad por parte del personal

ÍNDICE

1.ii.- AREA INVESTIGACIÓN Y FORMACIÓN. Gestión Personal

a) Base jurídica	RGPD: 6.1 a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. b) Tratamiento necesario para la ejecución de un contrato/ solicitud de servicios en el que el interesado es parte o para la aplicación de medidas precontractuales. c) Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. Ley 14/2007, de 3 de julio, de Investigación biomédica Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación Ley Orgánica 6/2001, de 21 de diciembre, de Universidades Decreto Legislativo 1/2013, de 8 de enero, Ley Andaluza de Universidades Estatutos de la propia Entidad Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Ley 1/2014, de trasparencia pública de Andalucía
b) Fines del tratamiento	Gestión y control de las actividades investigadoras, así como actividades y eventos promocionales y divulgativos. Gestión curricular. Gestión de titulaciones
c) Colectivo	Personal laboral y colaborador vinculado a la investigación y docencia
d) Categorías de Datos	Nombre y apellidos, DNI/NIF/Documento identificativo, dirección, teléfono, imagen, firma. Datos curriculares Datos económico-financieros: datos bancarios. Datos de seguros
e) Categoría destinatarios	Los datos podrán ser cedidos a las Administraciones vinculadas: SAS, UMA, así como otras con competencia en la materia. Los datos con finalidad administrativa serán comunicados a las entidades financieras, Agencia Estatal de la Administración Tributaria, Entidades aseguradoras.
f) Transf. Internacional	Posible comunicación/cesión a entidades organizadoras y vinculadas en actividades y eventos de investigación y docencia.
g) Plazo supresión	Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. Será de aplicación lo dispuesto en la normativa de archivos y documentación. Dado el carácter de actividad investigadora podrán permanecer en el histórico de la Entidad, y estar sujetos a las obligaciones de conservación de la normativa de investigación.
h) Medidas de seguridad	Las medidas de seguridad implantadas se corresponden con las previstas en el Reglamento Europeo 2016/679 de protección datos de carácter personal y L.O.P.D.G.D.D. 3/2018, y ENS Control de accesos y autorizaciones. Seguridad física infraestructuras y edificios Seguridad lógica de sistemas. Seguridad de redes Compromiso fehaciente de confidencialidad por parte del personal

1.iii.- AREA INVESTIGACIÓN Y FORMACIÓN. Gestión Formación

a) Base jurídica	RGPD: 6.1 a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. b) Tratamiento necesario para la ejecución de un contrato/ solicitud de servicios en el que el interesado es parte o para la aplicación de medidas precontractuales. c) Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. Ley Orgánica 6/2001, de 21 de diciembre, de Universidades Decreto Legislativo 1/2013, de 8 de enero, Ley Andaluza de Universidades Estatutos de la propia Entidad Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Ley 1/2014, de trasparencia pública de Andalucía
b) Fines del tratamiento	Gestión y control de las actividades formativas, así como actividades y eventos promocionales y divulgativos. Gestión curricular. Gestión de titulaciones
c) Colectivo	Personal laboral, alumnado y colaborador vinculado a la docencia

ÍNDICE

d) Categorías de Datos	Nombre y apellidos, DNI/NIF/Documento identificativo, dirección, teléfono, imagen, firma. Datos curriculares Datos económico-financieros: datos bancarios. Datos de seguros
e) Categoría destinatarios	Los datos podrán ser cedidos a las Administraciones vinculadas: SAS, UMA, así como otras con competencia en la materia. Los datos con finalidad administrativa serán comunicados a las entidades financieras, Agencia Estatal de la Administración Tributaria, Entidades aseguradoras.
f) Transf. Internacional	Posible comunicación/cesión a entidades organizadoras y vinculadas en actividades y eventos de investigación y docencia.
g) Plazo supresión	Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. Será de aplicación lo dispuesto en la normativa de archivos y documentación. Dado el carácter de actividad docente podrán permanecer en el histórico de la Entidad, bajo finalidad de gestión de titulaciones.
h) Medidas de seguridad	Las medidas de seguridad implantadas se corresponden con las previstas en el Reglamento Europeo 2016/679 de protección datos de carácter personal y L.O.P.D.G.D.D. 3/2018, y ENS Control de accesos y autorizaciones. Seguridad física infraestructuras y edificios Seguridad lógica de sistemas. Seguridad de redes Compromiso fehaciente de confidencialidad por parte del personal

2.- GESTIÓN DE RECURSOS HUMANOS

a) Base jurídica	RGPD: 6.1 a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. b) Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales. c) Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. Real Decreto Legislativo 2/2015, de 23 de octubre Ley del Estatuto de los Trabajadores. Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Ley 1/2014, de trasparencia pública de Andalucía.
b) Fines del tratamiento	Gestión de personal laboral. Expediente personal. Control horario. Formación. Prevención de riesgos laborales. Emisión de la nómina del personal, así como de todos los productos derivados de la misma. Gestión de la actividad sindical.
c) Colectivo	Personal laboral. Solicitantes
d) Categorías de Datos	Nombre y apellidos, DNI/CIF/Documento identificativo, número de registro de personal, número de Seguridad Social, dirección, firma y teléfono. Categorías especiales de datos: datos de salud (bajas por enfermedad, accidentes laborales y grado de discapacidad, sin inclusión de diagnósticos), afiliación sindical, a los exclusivos efectos de pagos de cuotas sindicales (en su caso), representante sindical (en su caso), justificantes de asistencia de propios y de terceros. Datos de características personales: Sexo, estado civil, nacionalidad, edad, fecha y lugar de nacimiento. Fecha de alta y baja, licencias, permisos y autorizaciones. Datos académicos y profesionales: Titulaciones, formación y experiencia profesional. Datos de detalle de empleo. Datos de control de presencia: fecha/hora entrada y salida, motivo de ausencia. Datos económico-financieros: Datos económicos de nómina. Datos bancarios.
e) Categoría destinatarios	Entidad a quien se encomiende la gestión en materia de riesgos laborales. Instituto Nacional de la Seguridad Social. Servicio Andaluz de Salud Organizaciones sindicales. Entidades financieras. Agencia Estatal de Administración Tributaria. Agencia Tributaria de Andalucía.
f) Transf. Internacional	No están previstas transferencias internacionales de los datos. No obstante, en la organización de eventos o desarrollo de trabajos de investigación, puede ser necesaria su comunicación.
g) Plazo supresión	Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. Será de aplicación lo dispuesto en la normativa de archivos y documentación.

ÍNDICE

	Los datos económicos de esta actividad de tratamiento se conservarán al amparo de lo dispuesto en la Ley 58/2003, de 17 de diciembre, General Tributaria.
h) Medidas de seguridad	Las medidas de seguridad implantadas se corresponden con las previstas en el Reglamento Europeo 2016/679 de protección datos de carácter personal y L.O.P.D.G.D.D. 3/2018, y ENS Control de accesos y autorizaciones. Seguridad física infraestructuras y edificios Seguridad lógica de sistemas. Seguridad de redes Compromiso fehaciente de confidencialidad por parte del personal

3.- GESTIÓN PRESUPUESTARIA Y ECONÓMICA

a) Base jurídica	RGPD: 6.1 a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. b) Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales. c) Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. Real Decreto Legislativo 2/2015, de la Ley del Estatuto de los Trabajadores. Ley 58/2003, de 17 de diciembre, General Tributaria. Estatutos de la Entidad Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Ley 1/2014, de trasparencia pública de Andalucía
b) Fines del tratamiento	Gestión de contabilidad y obligaciones fiscales y tributarias derivadas de la actividad de la Entidad.
c) Colectivo	Personal, proveedores, asociados
d) Categorías de Datos	Nombre y apellidos, DNI/NIF/Documento identificativo, dirección, firma y teléfono. Datos económicos, financieros y de seguros: Datos bancarios.
e) Categoría destinatarios	Entidades financieras. Entidades colaboradoras y vinculadas Instituto Nacional de la Seguridad Social. Agencia Estatal de Administración Tributaria. Agencia Tributaria de Andalucía
f) Transf. Internacional	No están previstas transferencias internacionales de los datos.
g) Plazo supresión	Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos, conforme a la Ley 58/2003, de 17 de diciembre, General Tributaria, además de los periodos establecidos en la normativa de archivos y documentación.
h) Medidas de seguridad	Las medidas de seguridad implantadas se corresponden con las previstas en el Reglamento Europeo 2016/679 de protección datos de carácter personal y L.O.P.D.G.D.D. 3/2018, y ENS Control de accesos y autorizaciones. Seguridad física infraestructuras y edificios Seguridad lógica de sistemas. Seguridad de redes Compromiso fehaciente de confidencialidad por parte del personal

4.- REGISTRO DE ENTRADA Y SALIDA

a) Base jurídica	RGPD: 6.1 a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. b) Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales. c) Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. Estatutos de la propia Entidad. Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Ley 1/2014, de trasparencia pública de Andalucía
b) Fines del tratamiento	Gestión del registro de entrada y salida de documentos de la entidad.

ÍNDICE

c) Colectivo	Personas físicas, incluidas representantes de personas jurídicas, que se dirigen a la entidad, o reciben comunicaciones de ella. Personal de la entidad destinatario o emisor de comunicaciones.
d) Categorías de Datos	Nombre y apellidos, DNI/NIF/Documento identificativo, dirección, teléfono y firma. Datos de representación en su caso. Datos relacionados con el documento presentado.
e) Categoría destinatarios	Sin cesiones previstas, se comunicarán a los distintos departamentos u órganos administrativos a los que, en su caso, se dirijan las distintas solicitudes o comunicaciones.
f) Transf. Internacional	No están previstas transferencias internacionales de los datos.
g) Plazo supresión	Se conservarán durante el tiempo que necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. Será de aplicación lo dispuesto en la normativa de archivos y documentación.
h) Medidas de seguridad	Las medidas de seguridad implantadas se corresponden con las previstas en el Reglamento Europeo 2016/679 de protección datos de carácter personal y L.O.P.D.G.D.D. 3/2018, y ENS Control de accesos y autorizaciones. Seguridad física infraestructuras y edificios Seguridad lógica de sistemas. Seguridad de redes Compromiso fehaciente de confidencialidad por parte del personal

5.- GESTIÓN DE COMUNICACIONES/WEB

a) Base jurídica	RGPD: 6.1 a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos b) Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales. Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Ley 1/2014, de trasparencia pública de Andalucía
b) Fines del tratamiento	Tramitación y resolución de solicitudes. Inscripción y gestión en actividades de las entidades. Envío de información corporativa. Gestión y seguimiento de requerimientos informativos.
c) Colectivo	Personas de contacto, personal laboral, asociados y otras entidades. Personas interesadas en las actividades e información de la Entidad.
d) Categorías de Datos	Nombre y apellidos, DNI/NIF/Documento identificativo, dirección, firma, teléfono, sector de actividad. Servicios solicitados
e) Categoría destinatarios	Sin cesión o comunicación predefinida, en principio no es necesaria, de serlo se recabaría el consentimiento preciso.
f) Transf. Internacional	No están previstas transferencias internacionales de los datos.
g) Plazo supresión	Los datos personales serán conservados durante la tramitación de los servicios requeridos. Los datos personales de las personas interesadas en la recepción de información comercial y empresarial, se mantendrán en el sistema de forma indefinida en tanto el interesado no solicite su supresión.
h) Medidas de seguridad	Las medidas de seguridad implantadas se corresponden con las previstas en el Reglamento Europeo 2016/679 de protección datos de carácter personal y L.O.P.D.G.D.D. 3/2018, y ENS Control de accesos y autorizaciones. Seguridad física infraestructuras y edificios Seguridad lógica de sistemas. Seguridad de redes Compromiso fehaciente de confidencialidad por parte del personal

ÍNDICE

6.- ACTIVIDADES de PROMOCIÓN

a) Base jurídica	RGPD: 6.1. b) Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales. e) Tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Estatutos de la propia Entidad Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Ley 1/2014, de trasparencia pública de Andalucía
b) Fines del tratamiento	Tramitación y resolución de eventos académicos, culturales y promocionales. Inscripción en actividades. Envío de información corporativa y comercial. Gestión de convenios de colaboración.
c) Colectivo	Participantes en las convocatorias de eventos y actividades. Personas interesadas en las actividades e información de la Entidad. Personas que firman los convenios en los que participa la Entidad
d) Categorías de Datos	Nombre y apellidos, DNI/NIF/Documento identificativo, dirección, firma, teléfono, sector de actividad. Participantes en eventos científicos. Datos de seguros. Hospedaje. Transporte Participantes en premios que llevan remuneración económica: datos bancarios. Firmantes de convenios: entidad a la que representan.
e) Categoría destinatarios	Participantes en convocatorias públicas: Los nombres y apellidos de los participantes en actividades podrán ser públicos, y estarán accesibles a través de la Web y redes sociales. Definido por aceptación de las bases y condiciones de las distintas actividades. Los datos personales de beneficiarios de premios y ayudas que lleven remuneración económica, serán comunicados a las entidades financieras, Agencia Estatal de la Administración Tributaria,
f) Transf. Internacional	Posible comunicación en eventos internacionales.
g) Plazo supresión	Los datos personales de los participantes en premios y ayudas serán conservados durante la tramitación del procedimiento de concesión de las mismas. Los datos económicos se conservarán al amparo de lo dispuesto en la Ley 58/2003, de 17 de diciembre, General Tributaria, y de la normativa de archivos y documentación. Los datos personales de las personas interesadas en la recepción de información comercial y empresarial, se mantendrán en el sistema de forma indefinida en tanto el interesado no solicite su supresión. Los datos personales de las personas inscritas en actividades generales serán suprimidos cuando éstas hubieran finalizado y no tuvieron participación activa y/o pública. Los datos personales de las personas inscritas en actividades y eventos públicos se mantendrán en el sistema de forma indefinida en tanto el interesado no solicite su supresión. Los datos personales de las personas que firman en representación de las entidades que suscriben convenios se mantendrán en el sistema de forma indefinida. Será de aplicación lo dispuesto en la normativa de archivos y documentación.
h) Medidas de seguridad	Las medidas de seguridad implantadas se corresponden con las previstas en el Reglamento Europeo 2016/679 de protección datos de carácter personal y L.O.P.D.G.D.D. 3/2018, y ENS Control de accesos y autorizaciones. Seguridad física infraestructuras y edificios Seguridad lógica de sistemas. Seguridad de redes Compromiso fehaciente de confidencialidad por parte del personal

7.- ASESORÍA JURÍDICA y CONTROL ÉTICO

a) Base jurídica	RGPD: 6.1 a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. b) Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales. c) Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

ÍNDICE

	e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Estatuto de los Trabajadores y estatutos de la propia Entidad. Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Ley 1/2014, de trasparencia pública de Andalucía Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción
b) Fines del tratamiento	Gestión y tramitación de asesoramiento jurídico. Canal de denuncias Seguimiento y ejecución de expedientes sancionadores, impugnaciones y ordenación del ámbito de la competencia. Cumplir y hacer cumplir la normativa deontológica y de funcionamiento
c) Colectivo	Solicitantes asesoramiento y sujetos de expedientes y reclamaciones.
d) Categorías de Datos	Datos identificativos: Nombre y apellidos. DNI/NIF, pasaporte y/o permiso de residencia. Direcciones de contacto: incluye teléfono, fax, e-mail y web, en su caso. Datos de características personales: Fecha y lugar de nacimiento. Nacionalidad. Sexo. Datos académicos y profesionales: Datos profesionales. Cargos corporativos. Datos vinculados al acto jurídico y canal de denuncias
e) Categoría destinatarios	Administración con competencia en el ámbito de ejecución. Entidades y organismos vinculados.
f) Transf. Internacional	No están previstas transferencias internacionales de los datos.
g) Plazo supresión	Se conservarán durante el tiempo que necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. Será de aplicación lo dispuesto en la normativa de archivos y documentación.
h) Medidas de seguridad	Las medidas de seguridad implantadas se corresponden con las previstas en el Reglamento Europeo 2016/679 de protección datos de carácter personal y L.O.P.D.G.D.D. 3/2018, y ENS Control de accesos y autorizaciones. Seguridad física infraestructuras y edificios Seguridad lógica de sistemas. Seguridad de redes Compromiso fehaciente de confidencialidad por parte del personal

8.- SEGURIDAD Y CONTROL DE INSTALACIONES

a) Base jurídica	RGPD: 6.1. c) Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. Estatutos de la propia Entidad.Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Ley 1/2014, de trasparencia pública de Andalucía
b) Fines del tratamiento	Garantizar la seguridad de personas, bienes e instalaciones. Registro y control de las visitas. Control laboral
c) Colectivo	Personal propio y externo que presta servicio en la entidad. Personas físicas o representantes de personas jurídicas que acuden a las sedes de la entidad a realizar diversas gestiones.
d) Categorías de Datos	De todo el colectivo de interesados: Imagen En relación al personal, el recogido en el control de acceso: Nombre y apellidos, DNI/NIF/Documento identificativo, dirección, teléfono. En su caso, datos de la representación que ostenta.
e) Categoría destinatarios	De ser necesario y requerido legalmente: Fuerzas y cuerpos de seguridad del Estado, órganos judiciales, organismos con competencia.
f) Transf. Internacional	No están previstas transferencias internacionales de los datos.
g) Plazo supresión	En un mes a contar desde la fecha de su recogida, de no mediar responsabilidades en las imágenes/información recogida.
h) Medidas de seguridad	Las medidas de seguridad implantadas se corresponden con las previstas en el Reglamento Europeo 2016/679 de protección datos de carácter personal y L.O.P.D.G.D.D. 3/2018, y ENS Control de accesos y autorizaciones. Seguridad física infraestructuras y edificios Seguridad lógica de sistemas. Seguridad de redes Compromiso fehaciente de confidencialidad por parte del personal

ÍNDICE

ANEXOS DOCUMENTALES

ANEXO A. DERECHOS DE LOS/LAS INTERESADOS/AS

Ejercicio de los derechos de los/las interesados/as. Los derechos de acceso a los datos personales, así como los de rectificación, cancelación, oposición, portabilidad y cuantos disponga la legislación vigente, son personalísimos y serán ejercidos por el/la afectado/a frente al responsable del fichero o DPD. Podrá, no obstante, actuar el/la representante legal de afectado/a cuando este/a se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos.

1. Derecho a consentir el tratamiento de datos personales

1.1. El/la interesado/a tiene derecho a que ninguno de sus datos personales sea tratado, a salvo las excepciones mencionadas, sin haber prestado con antelación su consentimiento, manifestado en cualquiera de las formas válidas en el ordenamiento jurídico español, y de forma que pueda ser acreditada su manifestación.
1.2. Los impresos de recogida de datos contendrán la cláusula de protección de datos correspondiente, que deberá ser suscrita por el/la interesado/a; o en el caso de formularios telemáticos, a través de firma digital o con el marcado de una casilla que desbloqueará el resto del documento de recogida telemática de datos.
1.3. En el caso de que los datos se recojan por medios no impresos, se advertirá al/a la, interesado/a de que su conversación será grabada, en el caso de sea posible hacerlo, y se le leerá la cláusula de protección de datos preguntándole sobre si da su conformidad para su tratamiento.
1.4. Tanto los impresos como las grabaciones se conservarán en el expediente correspondiente y formarán parte inseparable de él.
1.5. El consentimiento prestado podrá ser revocado cuando exista causa justificada para ello. Se informará de aquellos casos en los que la revocación no pueda tener efectos retroactivos.

2. Derecho de acceso. El/la interesado/a tendrá derecho a saber si la entidad está tratando o no datos personales que le conciernen y, de ser así, derecho de acceso a los mismos.
La **ENTIDAD** tendrá la obligación de facilitarle al, a la, interesado/a la siguiente información:

- Los fines del tratamiento.
- Las categorías de datos personales de que se trate.
- Los destinatarios/as o las categorías de destinatarios/as a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios/as en terceros u organizaciones internacionales. En estos últimos casos, se le informará de las garantías adecuadas relativas a la transferencia.
- De ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar ese plazo.
- La existencia del derecho a solicitar de la entidad la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al, a la, interesado/a, o a oponerse.
- El derecho a presentar una reclamación ante una autoridad de control.
- Cuando los datos no se hayan obtenido del, de la, interesado/a, cualquier información sobre su origen.
- La existencia de decisiones automatizadas, incluida la elaboración de perfiles, e información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el/la interesado/a.

La **ENTIDAD** facilitará una copia de los datos personales objeto del tratamiento al/a la, interesado/a, con la facultad de poder cobrar un canon razonable por cualquier otra copia solicitada basado en los costes administrativos. Dicha copia se facilitará por medio electrónico en un formato de uso común si la solicitud se presentó por estos medios, a menos que el/la interesado/a solicite que se le facilite de otro modo.

3. Derecho de rectificación. El/la interesado/a podrá solicitar a la **ENTIDAD** la rectificación de los datos personales inexactos que le conciernen, así como completar dichos datos teniendo en cuenta los fines del tratamiento. La **ENTIDAD** comunicará cualquier rectificación de los datos personales a cada uno de los/las destinatarios/as a los que se hayan comunicado dichos datos, en su caso, salvo que sea imposible o exija un esfuerzo desproporcionado.

ÍNDICE

4. Derecho de supresión o Derecho al Olvido. La **ENTIDAD** suprimirá sin dilación indebida los datos personales del, de la, interesado/a que así lo solicite cuando se den alguna de las circunstancias siguientes:

- Los datos personales ya no sean necesarios para los fines para los que fueron recogidos o tratados de otro modo;
- El/la interesado/a retire el consentimiento en el que se basa el tratamiento y este no se base en otro fundamento jurídico;
- El/la interesado/a se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento;
- Los datos personales hayan sido tratados ilícitamente;
- Los datos personales deban suprimirse en cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros aplicable a la entidad responsable;
- Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información a menores de 14 años.

La **ENTIDAD** suprimirá dichos datos cuando los haya hecho públicos, en la medida de lo posible, adoptando medidas razonables, atendiendo a la tecnología disponible y el coste de su aplicación, con miras a informar a los responsables que estén tratando los datos personales de la solicitud de supresión del, de la, interesado/a de cualquier enlace a esos datos, o cualquier copia de los mismos.

No se procederá a la supresión de los datos cuando el tratamiento sea necesario:

- Para ejercer el derecho a la libertad de expresión e información;
- Para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros aplicable a la entidad responsable del tratamiento, o el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos que le han sido conferidos
- Por razones de interés público en el ámbito de la salud pública;
- Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o para la formulación, el ejercicio o la defensa de reclamaciones.

La **ENTIDAD** comunicará cualquier supresión de datos personales a cada uno de los/las destinatarios/as a los que se hayan comunicado dichos datos, en su caso, salvo que sea imposible o exija un esfuerzo desproporcionado.

5. Derecho a la limitación del tratamiento. El/la interesado/a podrá solicitar a la **ENTIDAD** la limitación del tratamiento de sus datos personales. Dichos datos sólo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del, de la, interesado/a o para la formulación, ejercicio o defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

La limitación se producirá cuando se cumpla alguna de las siguientes condiciones:

- El/la interesado/a impugne la exactitud de los datos personales, durante el plazo necesario para que la entidad verifica la exactitud de los mismos;
- El tratamiento sea lícito y el interesado se oponga a la supresión de los datos personales, solicitando en su lugar la limitación de su uso;
- La **ENTIDAD** ya no necesite los datos personales para los fines del tratamiento, pero el/la interesado/a los necesite para la formulación, ejercicio o defensa de reclamaciones;
- El/la interesado/a se oponga al tratamiento, mientras se verifica si los motivos legítimos de la **ENTIDAD** prevalecen sobre los del, de la, interesado/a.

La **ENTIDAD** comunicará cualquier limitación de los datos personales a cada uno de los/las destinatarios/as a los que se hayan comunicado dichos datos, en su caso, salvo que sea imposible o exija un esfuerzo desproporcionado y además informará al, a la, interesado/a antes del levantamiento de la limitación de los datos personales cuando ésta haya tenido lugar.

6. Derecho a la portabilidad de los datos. La **ENTIDAD** entregará al, a la, interesado/a que lo solicite los datos personales que le haya facilitado, en un formato estructurado, de uso común y lectura mecánica, teniendo derecho a transmitirlos a otro responsable del tratamiento cuando:

- El tratamiento está basado en el consentimiento del, de la, interesado/a o en un contrato en el que el/la interesado/a es parte. En este supuesto, el/la interesado/a podrá solicitar a la entidad que transmita directamente los datos personales al otro responsable si es técnicamente posible,
- El tratamiento se realice por medios automatizados.

No procederá la portabilidad cuando el tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos a la **ENTIDAD**, ni cuando pueda afectar negativamente a los derechos y libertades de otros.

ÍNDICE

7. Derecho de oposición. El/la interesado/a podrá oponerse en cualquier momento al tratamiento de sus datos personales cuando dicho tratamiento se base en:

- El cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos a la entidad;
- La satisfacción de intereses legítimos perseguidos por la entidad o un tercero.

La **ENTIDAD** procederá al cese del tratamiento de dichos datos salvo que pueda acreditar motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, derechos y libertades del, de la, interesado/a, o para la formulación, ejercicio o defensa de reclamaciones.
Cuando el tratamiento tenga por objeto la realización de actividades de marketing directo, el/la interesado/a podrá oponerse en todo momento a dicho tratamiento, incluida la elaboración de perfiles.

8. Derecho a no ser objeto de decisiones individuales automatizadas. El/la interesado/a podrá ejercitar ante la **ENTIDAD** su derecho a no ser objeto de decisiones basadas únicamente en tratamientos automatizados, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de forma similar, excepto:

- Si la decisión es necesaria para la celebración o la ejecución de un contrato entre el/la interesado/a y la **ENTIDAD**,
- Si la decisión está autorizada por el Derecho de la Unión o de los Estados miembros que sea aplicable a la entidad y que establezca medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del, de la, interesado/a, o
- Si la decisión se basa en el consentimiento explícito del, de la, interesado/a.

En aquellos casos en que no corresponda la negativa del, de la, interesado/a., la **ENTIDAD** adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del, de la, interesado/a., como mínimo, el derecho a obtener la intervención humana en el tratamiento, a expresar su punto de vista y a impugnar la decisión adoptada.
La **ENTIDAD** no tomará decisiones basadas únicamente en el tratamiento automatizado de categorías especiales de datos personales, salvo consentimiento explícito del, de la, interesado/a. o que el tratamiento sea necesario por razones de interés público, y siempre que se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los legítimos intereses del, de la, interesado/a.

A.2.- Garantía de los derechos digitales

Los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España sea parte, son plenamente aplicables en Internet. Prestadores de servicios de la sociedad de la información y Proveedores de servicios de Internet contribuirán a garantizar su aplicación.

1.- Derecho a la neutralidad de Internet. Los/las usuarios/as tienen derecho a la neutralidad de Internet. Los/las proveedores/as de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos.

2.- Derecho de acceso universal a Internet. Toda persona tiene derecho a acceder a Internet independientemente de su condición personal, social, económica o geográfica. Se garantizará un acceso universal, asequible, de calidad y no discriminatorio para toda la población.

3.- Derecho a la seguridad digital. Los/las usuarios/as tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet. Los/las proveedores/as de servicios de Internet informarán a los/las usuarios/as de sus derechos.

4.- Derecho a la educación digital. El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales. Las Administraciones educativas deberán incluir en el diseño del bloque de asignaturas de libre configuración la competencia digital.

5.- Protección de los menores en Internet. Los padres, madres, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales. La utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor. En este sentido cabe señalar la Sentencia del Supremo de fecha 30 de junio de 2015:

> *La imagen, como el honor y la intimidad, constituye hoy un derecho fundamental de la persona consagrado en el artículo 18.1 de la Constitución, que pertenece a los derechos de la personalidad, con todas las características de estos derechos y que se concreta en la facultad exclusiva del titular de difundir o publicar su propia imagen pudiendo en consecuencia evitar o impedir la reproducción y difusión, con independencia de cuál sea la finalidad de esta difusión y que en el caso de menores tiene como presupuesto el hecho de que siempre que no medie el consentimiento de los padres o representantes legales de los menores con la ausencia del Ministerio Fiscal, la difusión de cualquier imagen de éstos ha de ser reputada contraria al ordenamiento jurídico (SSTS de 19 de noviembre de 2008 ; 17 de diciembre 2013 ; 27 de enero 2014, entre otras). Es en definitiva, es la propia norma la que objetiva el interés del menor y la que determina la consecuencia de su desatención.»*

Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del, de la, menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información. Cuando dicha publicación o difusión fuera a tener lugar a través de servicios de redes sociales o servicios equivalentes deberán contar con el consentimiento del menor o sus representantes legales (en caso de menores de 14 años).

6.- Derecho de rectificación en Internet. Toda persona tiene derecho a la libertad de expresión en Internet. Los/las responsables de redes sociales y servicios equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio del derecho de rectificación ante los/las usuarios/as que difundan contenidos que atenten contra el

ÍNDICE

derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz, atendiendo a los requisitos y procedimientos previstos en la Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación.

Cuando los medios de comunicación digitales deban atender la solicitud de rectificación formulada contra ellos deberán proceder a la publicación en sus archivos digitales de un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual de la persona. Dicho aviso deberá aparecer en lugar visible junto con la información original.

7.- Derecho a la actualización de informaciones en medios de comunicación digitales. Toda persona tiene derecho a solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible junto a las noticias que le conciernan cuando la información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación, causándole un perjuicio.

En particular, procederá la inclusión de dicho aviso cuando las informaciones originales se refieran a actuaciones policiales o judiciales que se hayan visto afectadas en beneficio del interesado como consecuencia de decisiones judiciales posteriores. En este caso, el aviso hará referencia a la decisión posterior.

8.- Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral. Los/las trabajadores/as y los/las empleados/as públicos/as tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.

El/la empleador/a podrá acceder a los contenidos derivados del uso de medios digitales facilitados al personal laboral a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos. Los/las empleados/as deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los/las representantes de los/las trabajadores/as.

El acceso por el/la empleador/a al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los/las trabajadores/as, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados. Los/las trabajadores/as deberán ser informados/as de los criterios de utilización a los que se refiere este apartado.

9.- Derecho a la desconexión digital en el ámbito laboral. Los/las trabajadores/as y los/las empleados/as públicos/as tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los/las representantes de los/las trabajadores7as.

El/la empleador/a, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia, así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

10.- Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo. Los/las empleadores/as podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de trabajadores/as o empleados/as públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los/las empleadores/as habrán de informar con carácter previo, y de forma expresa, clara y concisa, a trabajadores/as o empleados/as públicos y, en su caso, a sus representantes, acerca de esta medida.

En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por trabajadores/as o empleados/as públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica. En ningún caso se admitirá la instalación de sistemas de

grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de trabajadores/as o empleados/as públicos, tales como vestuarios, aseos, comedores y análogos.

La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley.

11.- Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral. Los/las empleadores/as podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de trabajadores/as o empleados/as públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Con carácter previo, los/las empleadores/as habrán de informar de forma expresa, clara e inequívoca a trabajadores/as o empleados/as públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

12.- Derechos digitales en la negociación colectiva. Los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de trabajadores/as y la salvaguarda de derechos digitales en el ámbito laboral.

13.- Derecho al olvido en búsquedas de Internet. Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información. Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el/la afectado/a evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet. Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo.

El ejercicio del derecho al que se refiere este artículo no impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho.

14.- Derecho al olvido en servicios de redes sociales y servicios equivalentes. Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes.

Toda persona tiene derecho a que sean suprimidos los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información. Del mismo modo deberá procederse a la supresión de dichos datos cuando las circunstancias personales que en su caso invocase el/la afectado/a evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio. Se exceptúan de lo dispuesto en este apartado los datos que hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.

En caso de que el derecho se ejercitase por un/una afectado/a respecto de datos que hubiesen sido facilitados al servicio, por él/ella o por terceros, durante su minoría de edad, el/la prestador/a deberá proceder sin dilación a su supresión por su simple solicitud, sin necesidad de que concurran las circunstancias mencionadas en el apartado 2.

15.- Derecho de portabilidad en servicios de redes sociales y servicios equivalentes. Los/las usuarios/as de servicios de redes sociales y servicios de la sociedad de la información equivalentes tendrán derecho a recibir y transmitir los contenidos que hubieran facilitado a los prestadores de dichos servicios, así como a que los prestadores los transmitan directamente a otro prestador designado por el usuario, siempre que sea

técnicamente posible. Los/las prestadores/as podrán conservar, sin difundirla a través de Internet, copia de los contenidos cuando dicha conservación sea necesaria para el cumplimiento de una obligación legal.

16.- Derecho al testamento digital. El acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas se regirá por las siguientes reglas:
a) Las personas vinculadas al/la fallecido/a por razones familiares o de hecho, así como sus herederos/as podrán dirigirse a los/las prestadores/as de servicios de la sociedad de la información al objeto de acceder a dichos contenidos e impartirles las instrucciones que estimen oportunas sobre su utilización, destino o supresión.
Como excepción, las personas mencionadas no podrán acceder a los contenidos del/de la causante, ni solicitar su modificación o eliminación, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los/las herederos/as a acceder a los contenidos que pudiesen formar parte del caudal relicto.
b) El/la albacea testamentario/a así como aquella persona o institución a la que el/la fallecido/a hubiese designado expresamente para ello también podrá solicitar, con arreglo a las instrucciones recibidas, el acceso a los contenidos con vistas a dar cumplimiento a tales instrucciones.
c) En caso de personas fallecidas menores de edad, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.
d) En caso de fallecimiento de personas con discapacidad, estas facultades podrán ejercerse también, además de por quienes señala la letra anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

Las personas legitimadas en el apartado anterior podrán decidir acerca del mantenimiento o eliminación de los perfiles personales de personas fallecidas en redes sociales o servicios equivalentes, a menos que el/la fallecido/a hubiera decidido acerca de esta circunstancia, en cuyo caso se estará a sus instrucciones. El/la responsable del servicio al que se le comunique, con arreglo al párrafo anterior, la solicitud de eliminación del perfil, deberá proceder sin dilación a la misma.

PROTOCOLO DE ACTUACIÓN EN EL EJERCICIO DE DERECHOS

1.- Introducción.

El Reglamento EU 2016/679 y la L.O.P.D.G.D.D. 3/2018 de Protección de Datos de Carácter Personal y Garantías de Derechos Digitales, establecen las obligaciones y responsabilidades que los/las responsables y encargados/as de tratamiento deben desarrollar con el fin de garantizar los derechos de las personas en el ámbito del tratamiento de datos de carácter personal.

2.- Disposiciones comunes a los derechos: Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado (art.12)

Con carácter general, los/las responsables deben facilitar a los/las interesados/as el ejercicio de sus derechos, así como los procedimientos y las formas para ello deben ser visibles, accesibles y sencillas. La información podrá facilitarse por escrito o por otros medios, inclusive, por medios electrónicos, especialmente cuando el tratamiento se realiza por estos medios.

El ejercicio de los derechos será gratuito para el/la interesado/a, salvo cuando: casos en que se formulen solicitudes manifiestamente infundadas o excesivas, especialmente por repetitivas, el/la responsable podrá cobrar un canon que compense los costes administrativos de atender a la petición o negarse a actuar (el canon no podrá implicar un ingreso adicional para el/la responsable, sino que deberá corresponderse efectivamente con el verdadero coste de la tramitación de la solicitud).

Cuando el/la interesado/a presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el/la interesado/a solicite que se facilite de otro modo.

2.1.- Plazos: El/la responsable deberá informar al/la interesado/a sobre las actuaciones derivadas de su petición en el plazo de un mes (podrá extenderse dos meses más cuando se trate de solicitudes especialmente complejas y deberá notificar esta ampliación dentro del primer mes).

Si el/la responsable decide no atender una solicitud, deberá informar de ello, motivando su negativa, dentro del plazo de un mes desde su presentación.

2.2.- Acreditación de la personalidad o representación: En virtud del RGPD los/las responsables deberán tomar medidas para verificar la identidad de quienes ejerzan sus derechos.

La acreditación de la personalidad del/de la interesado/a puede realizarse mediante exhibición de DNI u otro documento válido o la remisión de fotocopia adjunta a la solicitud. También es posible acreditar la identidad mediante firma electrónica cuando el procedimiento de ejercicio de derechos se realice de forma telemática.

En el caso de representación, ya sea legal o voluntaria, deberá aportarse el documento que acredite la representación, junto con fotocopia del/de la representado/a.

Ejercicio de derechos ante el/la encargado/a del tratamiento: El/la responsable podrá contar con la colaboración de los/las encargados/as de tratamiento para atender al ejercicio de derechos de los/las interesados/as, pudiendo incluir esta colaboración en el contrato de encargo de tratamiento.

2.3.- Requisitos de la solicitud: Petición dirigida a la Entidad, responsable del tratamiento, mediante cualquier medio que garantice la identificación del/de la afectado/a, titular de los datos (DNI, firma electrónica u otro medio análogo) y, en su caso, identificación de la persona que lo/la represente junto con el documento que acredite tal representación y la identidad del/de la representante.

Salvo en casos de especial complejidad, el/la afectado/a está facultado/a para referirse en su consulta tanto a datos concretos o a la totalidad de los datos sometidos a tratamiento por parte del/de la Responsable de los datos. Pese a lo anterior, en caso de que cualquiera de las entidades a las que se dirijan la solicitud del/de la interesado/a, traten una gran cantidad de información sobre un/a interesado/a, se podrá pedir a éste que especifique la información a que se refiere su solicitud de acceso.

La petición en que se concreta la solicitud deberá contener a su vez el domicilio a efectos de notificaciones, fecha y firma del/de la solicitante, acompañando fotocopia del DNI o documento equivalente, así como autorización del representado y DNI del/de la representante o documento equivalente.

3.- ¿Qué debe hacer el/la Responsable del Tratamiento? Ante una solicitud de ejercicio de derechos, el/la Responsable del tratamiento, resolverá en el plazo máximo de un mes a contar desde la recepción de la solicitud. En este sentido, la persona de la entidad, que reciba la solicitud deberá observar, en primer lugar, cuándo ha llegado la solicitud, haciéndolo constar en la misma, así como el tiempo que resta para la finalización del plazo, poniéndolo sin dilación en conocimiento de DPD, y del/de la responsable de la entidad. De la contestación, de su negativa o imposibilidad, también se informará a efectos de su seguimiento. Lo anterior, sin perjuicio de proceder a su tramitación.

La solicitud deberá ser cursada por el Departamento al que corresponda el tratamiento, a efectos de su cumplimentación y contestación, con el asesoramiento del DPD, en el plazo de un mes.

El/la Responsable del tratamiento, deberá contestar la solicitud que se le dirija, con independencia de que se lleven a cabo tratamientos de datos del/de la interesado/a, debiendo utilizar cualquier medio fehaciente que permita acreditar el contenido de la respuesta que se remite y la fecha de su recepción por el/la destinatario/a. En el caso de que la solicitud no reúna los requisitos descritos anteriormente, el/la Responsable deberá solicitar al/a la interesado/a la subsanación de los mismos.
Asimismo, la información que deberá aportar el/la Responsable comprenderá:

a. Los datos o categorías de datos del/de la afectado/a y los resultantes de cualquier elaboración o proceso de los mismos,
b. El origen de los datos,
c. Las comunicaciones realizadas o que se prevean realizar (incluido los/las destinatarios/as o categorías de destinatarios),
d. La especificación de las finalidades para los que se almacenarán los datos,
e. Si es posible, el plazo previsto de conservación de los datos o los criterios utilizados para determinar este plazo,
f. El derecho a presentar una reclamación ante una autoridad de control,
g. La existencia de decisiones automatizadas, incluida la elaboración de perfiles e información significativa sobre la lógica aplicada, así como la importancia y consecuencias para el/la interesado/a.
h. Las garantías adecuadas respecto a las transferencias internacionales que se produzcan.

ÍNDICE

La información se facilitará de modo perfectamente comprensible, sin usar códigos o claves que requieran el uso de dispositivos mecánicos específicos. En los supuestos de solicitudes excesivas, reiterativas, o improcedentes la empresa podrá fijar un canon para cursar la respuesta, como gastos de gestión.

4.- Los Derechos.

4.3.- Derecho de acceso. Concepto. (art.15): El derecho de acceso se refiere al derecho a conocer si el/la responsable está tratando datos del/de la interesado/a. En caso afirmativo, el/la interesado/a deberá ser informado/a acerca del tipo de datos tratados, la finalidad, destinatarios, plazo de conservación, origen y transferencias internacionales.

Contestación.:

a) Otorgamiento del acceso: El derecho de acceso será atendido, independientemente de que la organización disponga o no de datos del/de la solicitante, dentro del plazo de un mes a contar desde el momento de su recepción (a excepción de los supuestos comentados en el apartado 2).

Si la organización estuviese tratando datos del/de la solicitante, deberá facilitar una copia de los datos personales objeto de tratamiento. El/la responsable podrá percibir por cualquier otra copia solicitada por el/la interesado/a un canon razonable basado en los costes administrativos.

Cuando el/la interesado/a presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

b) Denegación del acceso: El RGPD no establece ningún supuesto de denegación del acceso en el ejercicio del derecho de acceso.

4.4- Derecho de rectificación. El derecho de rectificación es el derecho del/de la afectado/a a que se modifiquen los datos que resulten ser inexactos o incompletos (art.16)

La solicitud de rectificación deberá indicar a qué datos se refiere, así como la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado.

El/la Responsable del tratamiento deberá comunicar cualquier rectificación a cada uno de los/las destinatarios/as a los que se hayan comunicado los datos personales.

Contestación. El RGPD establece que el/la interesado/a tendrá derecho a obtener sin dilación indebida del/de la responsable del tratamiento la rectificación de los datos personales inexactos que le afectan.

Asimismo, el/la responsable del tratamiento comunicará cualquier rectificación de datos personales a cada uno de los/las destinatarios/as a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado.

El/la responsable informará al/a la interesado/a acerca de dichos destinatarios, si este/a así lo solicita.

4.5.- Derecho de supresión («el derecho al olvido»). El Derecho al olvido tiene su fundamento en el derecho de borrado de datos personales.

El/la responsable del tratamiento que ha hecho públicos los datos personales se le impone la obligación de informar a los/las demás responsables que estén tratando los datos, la obligación de borrar cualquier enlace, copia o repetición de los datos personales.

El/la responsable del tratamiento deberá tomar medidas razonables, teniendo en cuenta la tecnología disponible y los medios de que disponga, incluyendo medidas técnicas, para informar a los responsables, que están tratando los datos, de la solicitud del/de la interesado/a.

El/la responsable del tratamiento deberá comunicar cualquier supresión a cada uno de los/las destinatarios/as a los que se hayan comunicado los datos personales (art.17)

El RGPD establece que los/las interesados/as deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los/las interesados/as han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el Reglamento.

Existe obligación de suprimir y borrar los datos personales en los siguientes supuestos:

1. Datos que ya no son necesarios en relación con la finalidad que fueron recogidos.
2. El/la interesado/a retira el consentimiento del tratamiento con base a que dicho consentimiento fue prestado de forma voluntaria, mediante consentimiento expreso y ahora tiene el mismo derecho de retirarlo.
3. Oposición al tratamiento de datos personales.
4. Que los datos personales hayan sido tratados ilegalmente.
5. Datos borrados por el cumplimiento de una obligación legal en Derecho de la UE o del Estado Miembro al que esté sujeto el responsable.
6. Los datos de un/a menor de 16 años recogidos con la autorización de los padres/madres/tutores.
7. No se aplicará el derecho al olvido cuando los datos personales sean necesarios para alguno de los siguientes supuestos:
8. Ejercicio del derecho a la libertad de expresión e información. Especialmente respecto a noticias relativas a personajes públicos o de interés público.
9. Cuando tenga por finalidad cumplir con una obligación legal (derecho UE o de un Estado
10. Miembro) que requiera el tratamiento de datos personales para cumplir con una misión de interés público o por ser inherente al ejercicio del poder público.
11. Por razones de interés público en el ámbito de la salud pública.
12. Con fines de archivo, interés público, fines de investigación científica, e históricos o fines estadísticos.
13. Para la formulación, el ejercicio o la defensa de reclamaciones.

Contestación. A este derecho se le aplican los mismos plazos y procedimientos que a los restantes derechos previstos en el RGPD.

El/la responsable del tratamiento comunicará cualquier supresión de datos personales efectuada a cada uno/a de los/las destinatarios/as a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El/la responsable informará al/a la interesado/a acerca de dichos destinatarios, si este/a así lo solicita.

4.6.- Derecho a la limitación del tratamiento. La limitación de tratamiento supone que, a petición del/de la interesado/a, no se aplicarán a sus datos personales las operaciones de tratamiento que cada caso corresponderían (art.18). El RGPD prevé varios supuestos en los que se podría ejercitar:

- ✓ Cuando el consentimiento para el tratamiento no sea necesario porque concurra un motivo legítimo y fundado que lo justifique.
- ✓ Cuando se trate de ficheros cuya finalidad sea la realización de actividades de publicidad y prospección comercial independientemente de quien lo haya creado.
- ✓ Cuando el tratamiento tenga por finalidad la adopción de una decisión basada en un tratamiento automatizado de los datos de carácter personal del afectado.

Solicitud. Se puede solicitar la limitación cuando:

- El/la interesado/a ha ejercido los derechos de rectificación u oposición y el/la responsable está en proceso de determinar si procede atender a la solicitud.
- El tratamiento es ilícito, lo que determinaría el borrado de los datos, pero el/la interesado/a se opone a ello.
- Los datos ya no son necesarios para el tratamiento, que también determinaría su borrado, pero el/la interesado/a solicita la limitación porque los necesita para la formulación, el ejercicio o la defensa de reclamaciones.

En el tiempo que dure la limitación, el/la responsable sólo podrá tratar los datos afectados, más allá de su conservación:

- ➢ Con el consentimiento del/de la interesado/a.
- ➢ Para la formulación, el ejercicio o la defensa de reclamaciones.
- ➢ Para proteger los derechos de otra persona física o jurídica.
- ➢ Por razones de interés público importante de la Unión o del Estado miembro correspondiente.

Contestación. A este derecho se le aplican los mismos plazos y procedimientos que a los restantes derechos previstos en el RGPD.

El/la responsable del tratamiento comunicará cualquier limitación del tratamiento efectuada a cada uno de los/las destinatarios/as a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El/la responsable informará al/a la interesado/a acerca de dichos destinatarios, si este así lo solicita.

4.7.- Derecho a la portabilidad de los datos. El/la interesado/a tiene derecho a transmitir sus datos a otro/a responsable sin obstáculos por parte del/ de la responsable al cual le han sido proporcionados, cuando:

- El tratamiento se basa en el consentimiento.
- El tratamiento se haga a través de medios automatizados.

En el ejercicio de su derecho a la portabilidad de los datos, el/la interesado/a tiene derecho a que los datos sean transmitidos directamente desde el/la responsable a otro/a responsable, siempre que sea técnicamente factible (art.20)

Este derecho no es aplicable:

- ✓ A los datos de terceras personas que un/a interesado/a haya facilitado a un/a responsable.
- ✓ En caso de que el/la interesado/a haya solicitado la portabilidad de datos que le incumban pero que hayan sido proporcionados a responsable por terceros.

4.8.- Derecho de oposición y decisiones individuales automatizadas. El/la interesado/a tendrá derecho a oposición, en cualquier momento, por motivos relacionados con su situación particular sobre aquellos datos personales suyos que sean objeto de un tratamiento.

El/la responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del/de la interesado/a, o para la formulación, el ejercicio o la defensa de reclamaciones (art.21)

Derecho de oposición a las decisiones automatizadas (Ej. la elaboración de perfiles): Los/las interesados/as tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos/as o que les afecte de manera significativa, que se base únicamente en tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como rendimiento laboral, crédito, fiabilidad o conducta (art.22)

Excepciones al ejercicio del derecho de oposición (tratamiento automatizado):

- ➢ Es necesario para el cumplimiento de un contrato entre el/la interesado7a y el/la responsable del tratamiento.
- ➢ Se encuentra autorizado por ley.
- ➢ Cuenta con el consentimiento explícito del/de la interesado/a.

Derecho de oposición en tratamientos de Marketing directo: Cuando los datos personales sean tratados con fines de marketing directo, el/la interesado/a tiene derecho a oponerse en cualquier momento a dicho tratamiento.

A más tardar en el momento de la primera comunicación con el/la titular de los datos, se informará del derecho a ejercer su derecho de oposición.

Se deberá informar de manera explícita a la atención de la persona interesada y se presentará de manera clara y separada de cualquier otra información.

Contestación. El RGPD no se pronuncia al respecto. Aunque se presume que, por analogía, el/la interesado/a tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la oposición de los datos personales que le conciernan.

FORMULARIO PARA EL EJERCICIO DE DERECHOS

En……., a…. de ……de 20…

DATOS RESPONSABLE DEL TRATAMIENTO

Fundación para la Investigación de Málaga en Biomedicina y Salud -FIMABIS-
Instituto de Investigación Biomédica de Málaga y Plataforma en Nanomedicina -IBIMA Plataforma BIONAND-
C.I.F.: G29830643
Parque Tecnológico de Andalucía (PTA)Avenida Severo Ochoa, 35, 29590, Málaga.
tlf. 951 440 260- 951 440 263; fimabis@fimabis.org / ibima@ibima.eu

Delegado Protección de Datos: José Montilla Chicano, DPD_ProteccionDatos@ibima.eu

DATOS SOLICITANTE

D./D.ª_____DNI._____
Dirección:_____nº_____
Localidad:_____CP_____Provincia:_____
Tlf.:_____Email:_____

DATOS REPRESENTANTE LEGAL (si fuese necesario)

D./D.ª_____DNI._____
Dirección:_____nº_____
Localidad:_____CP_____Provincia:_____
Tlf.:_____Email:_____

DATOS DE NOTIFICACIÓN:

Especifique cómo desea que le respondamos a su solicitud:
☐ Por medios electrónicos (email).
☐ Correo postal (en la dirección indicada en los datos de contacto).

Por medio del presente escrito, y de acuerdo con lo establecido por la legislación vigente, manifiesta su deseo de **EJERCER SU DERECHO** (señale en su caso el derecho a ejercer, en el reverso, o a continuación, de este formulario encontrará una breve descripción de los derechos)

☐ **ACCESO** ☐ **RECTIFICACION**
☐ **SUPRESION** ☐ **LIMITACION DEL TRATAMIENTO**
☐ **PORTABILIDAD DE LOS DATOS** ☐ **OPOSICION**

INFORMACIÓN ADICIONAL (*En este espacio puede escribir toda la información que desee sobre el ejercicio de su derecho*).

_____
_____

DOCUMENTACIÓN QUE ACOMPAÑA

☐ **COPIA DNI SOLICITANTE (obligatoria)**
☐ **COPIA DNI REPRESENTANTE (en caso de representación)**
☐ **OTRA.**_____

Firmado Solicitante: *Firmado Representante*

* copia en blanco y negro y/o con marca que impida su reproducción fraudulenta
En el caso de menores de 14 años, debe ser firmado con representación fehaciente

ÍNDICE

EXPLICACIÓN SOBRE LOS DERECHOS: (*Reverso documento*)

DERECHO DE ACCESO: Al ejercer este derecho se solicita que se facilite gratuitamente el derecho de acceso al Tratamiento de Datos Personales en el plazo máximo de un mes a contar desde la recepción de esta solicitud, que se le remita a la dirección arriba indicada por correo toda la información relacionada en el art. 15 del RGPD, de modo legible e inteligible y dentro del plazo indicado.
DERECHO DE RECTIFICACION: Al ejercer este derecho se solicita que se facilite gratuitamente el derecho de rectificación, de conformidad con lo previsto en el art. 16 del RGPD. Será necesario aportar los correspondientes justificantes.
DERECHO DE SUPRESION: Al ejercer este derecho se solicita que se facilite gratuitamente el derecho de supresión, o derecho al olvido, de conformidad con lo previsto en el art. 17 del RGPD. Será necesario aportar los correspondientes justificantes.
DERECHO A LA LIMITACION DEL TRATAMIENTO: Al ejercer este derecho se solicita que se facilite gratuitamente el derecho a la limitación del tratamiento indicado, de conformidad con lo previsto en los arts. 18 y 19 del RGPD. Será necesario aportar los correspondientes justificantes.
DERECHO A LA PORTABILIDAD DE LOS DATOS: Al ejercer este derecho se solicita que se le facilite gratuitamente a la limitación del tratamiento indicado, de conformidad con lo previsto en el art. 20 del RGPD.
DERECHO DE OPOSICION: Al ejercer este derecho se solicita que se le facilite gratuitamente a la limitación del tratamiento indicado, de conformidad con lo previsto en los arts. 21 y 22 del RGPD. Será necesario aportar los correspondientes justificantes.

Al ejercer cualquiera de estos derechos se solicita que, en caso de que se acuerde, dentro del plazo de un mes, que no procede atender total o parcialmente el derecho ejercido, se comunique motivadamente a fin de, en su caso, **solicitar la tutela de la Agencia Española de Protección de Datos**, al amparo del art. 57 del RGPD. Opcionalmente, y previo a la reclamación ante la Agencia Española de Protección de Datos, si considera que el/la responsable del tratamiento no ha satisfecho correctamente sus derechos, puede solicitar una valoración ante el Delegado de Protección de Datos al que corresponda de acuerdo al tratamiento objeto del derecho.

ÍNDICE

ANEXO B.- PROTOCOLO DE GESTIÓN DE INCIDENCIAS

OBJETIVO: El Objetivo del presente documento es establecer y comunicar a todas las áreas de la entidad, el procedimiento para notificar y gestionar de manera estándar los incidentes que puedan comprometer la seguridad de los Datos de Carácter Personal, en cumplimiento del Reglamento EU 2016/679. En este sentido, establece que los incidentes de seguridad que afecten a Datos de Carácter Personal e Información deben ser documentados y notificados.

ALCANCE: El presente protocolo es de aplicación a todos los departamentos/comisiones y personal con acceso a la información de la entidad, indistintamente del medio o formato de tratamiento.

PROCEDIMIENTO: El presente procedimiento se ejecutará ante cualquier incidente que afecte a la seguridad de los datos de carácter personal. En cualquier caso, se llevarán a cabo las acciones descritas: "Comunicación del Incidente", "Registro del Incidente" y "Evaluación del Incidente", ejecutándose las acciones descritas en "Notificación del Incidente" en los casos en que el incidente de seguridad suponga un riesgo alto para los derechos y libertades de los afectados.

COMUNICACIÓN: Todo el personal está obligado a comunicar cualquier incidencia de seguridad relativa a los datos de carácter personal al Responsable de Seguridad, responsable de Seguridad Informática y al Delegado de Protección de Datos. Dicha notificación se realizará mediante los buzones de correo electrónico de dichos responsables, bien directamente o bien través del formulario facilitado.

Las incidencias pueden aparecer en todas las actividades relacionadas con el manejo y gestión de información en formato físico o bases de datos lógicas que almacenen datos de carácter personal, así como en el desarrollo de las actividades que afecten a la seguridad de los datos contenidos en las mismas.
A continuación, se citan algunos ejemplos de incidencias:

- Crear una base de datos de carácter personal sin autorización de responsable.
- Recabar datos de carácter personal sin la autorización de afectado/a y sin informarle de sus derechos.
- Uso de los datos de carácter personal con una finalidad diferente a la registrada en su recogida.
- Intento o violación del control de acceso físico y de bases de datos.
- Alterar bases de datos (borrado, modificación o inclusión de datos no correspondientes).
- Sacar datos en soportes sin la autorización pertinente.
- Sacar datos en soportes diferentes a los autorizados en el registro de la base de datos.
- Transferir datos sin el preceptivo contrato que lo legitime
- Incumplir lo establecido para la recuperación de datos.
- Incumplir los plazos establecidos para resolver y contestar las solicitudes para ejercer los derechos de interesados/as.
- Usar ilícitamente datos de carácter personal.
- Ejecutar el proceso de recuperación de datos.
- Gestionar incorrectamente los backups.
- Perdida de activo material (Teléfono de trabajo, portátiles, etc).
- Imposibilidad de acceder al sistema con nuestro usuario/contraseña habitual.
- Contraseña de acceso posiblemente comprometida.
- Comportamiento anormal del sistema (información incompleta o irreal, fallos inesperados, etc.).

Las incidencias relativas a datos de carácter personal no se limitan al tratamiento automatizado, sino que también incluyen los medios de tratamiento no automatizado. Así pues, las incidencias que afecten a dichos medios, como por ejemplo la pérdida de listados en papel con datos de carácter personal, deberán ser también obligatoriamente reportadas y registradas por el sistema descrito en el presente apartado.

ÍNDICE

REGISTRO: Una vez se ha tenido constancia o conocimiento del incidente de seguridad, se comunicará inmediatamente al/la Responsable de Seguridad, Responsable de Seguridad Informática y al DPD, recogiendo de forma detallada:

- Tipo de Incidencia.
- Descripción de la Incidencia.
- Fecha y hora de la notificación.
- Usuario/a que reporta la incidencia.

EVALUACIÓN: Una vez se ha registrado el incidente de seguridad, el/la Responsables de Seguridad y DPD se encargarán de evaluar el incidente de seguridad.
En caso de que se considere oportuno, en base a la criticidad del incidente, podrá convocar a los/las responsables departamentales involucrados con el fin de evaluar el impacto del incidente en el grupo.
La categoría o nivel de criticidad del incidente respecto a la seguridad de la información afectada. Siguiendo la clasificación genérica, podemos distinguir entre:

1. Crítico (afecta a datos valiosos, gran volumen y en poco tiempo)
2. Muy Alto (Cuando dispone de capacidad para afectar a información valiosa, en cantidad apreciable)
3. Alto (Cuando dispone de capacidad para afectar a información valiosa)
4. Medio (Cuando dispone de capacidad para afectar a un volumen apreciable de información)
5. Bajo (Escasa o nula capacidad para afectar a un volumen apreciable de información).

Adicionalmente pueden existir escenarios técnicos que pueden dar lugar a un incidente, el/la responsable de seguridad informática estará vigilante e informará inmediatamente de dichas circunstancias (ataques, códigos maliciosos, etc.).
El/la responsable y DPD, analizarán las consecuencias y determinarán su comunicación a la Autoridad de control y/o afectados/as

NOTIFICACIÓN

Notificación a la Autoridad de control: Como se ha comentado anteriormente, tan pronto como el/la Responsable del tratamiento tenga conocimiento de que se ha producido una brecha de la seguridad de los datos personales debe, sin dilación y, a más tardar en las 72 horas siguientes a tener constancia, efectuar la correspondiente notificación a la Autoridad de Control. Se considera que se tiene constancia de una brecha de seguridad cuando hay una certeza de que se ha producido y se tiene conocimiento suficiente de su naturaleza y alcance.

El criterio a tener en cuenta para determinar si un incidente ha producido “una brecha de la seguridad de los datos personales” se recoge en el propio RGPD, e incluye “todas aquellas brechas de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Esta comunicación se realizará con el modelo de comunicación dispuesto por la Autoridad de control, y deberá contener la siguiente información:

- Datos identificativos y de contacto de:
- Entidad / Responsable del tratamiento
- DPD (si está designado) o persona de contacto.

ÍNDICE

- Indicación de si se trata de una notificación completa o parcial. En caso de tratarse de una notificación parcial indicar si se trata de una primera notificación o una notificación complementaria.

Información sobre la brecha de seguridad de datos personales:

- Fecha y hora en la que se detecta.
- Fecha y hora en la que se produce el incidente y su duración.
- Circunstancias en que se haya producido la brecha de seguridad de datos personales (por ejemplo, pérdida, robo, copia, etc.)
- Naturaleza y contenido de los datos personales en cuestión.
- Resumen del incidente que ha causado la brecha de seguridad de datos personales (con indicación de la ubicación física y del soporte de almacenamiento).
- Posibles consecuencias y efectos negativos en los afectados.
- Medidas técnicas y organizativas que se hayan adoptado por parte del responsable del tratamiento según el apartado 33.2d) del RGPD.
- Categoría de los datos afectados y número de registros afectados
- Categoría y número de individuos afectados/as
- Posibles cuestiones de carácter transfronterizo, indicando la posible necesidad de notificar a otras autoridades de control.

Si en el momento de la notificación, no fuese posible facilitar toda la información, podrá facilitarse posteriormente, de manera gradual en distintas fases. La primera notificación se realizará en las primeras 72h, y al menos se realizará una comunicación final o de cierre cuando se disponga de toda la información relativa al incidente.

Cuando el/la Responsable del tratamiento realice la primera notificación deberá informar si proporcionará más información a posteriori. También podrá aportar información adicional mediante comunicaciones intermedias a la autoridad de control bajo petición de esta, o cuando el responsable considere adecuado actualizar la situación de la misma.

Cuando la notificación inicial no sea posible en el plazo de 72 horas, la notificación deberá realizarse igualmente a posteriori, y en ella deberán constar y justificarse los motivos de la dilación.
Las notificaciones deben ser sean claras, concisas y que incluyan la información necesaria para que puedan ser analizadas adecuadamente.

Notificación a los afectados/as: Al igual que en el aparatado anterior, en el caso de que se produzca un incidente de seguridad que suponga un riesgo alto para los derechos y libertades de los afectados/as, este deberá comunicarse a los/las afectados/as con el objetivo de permitir a estos la toma de medidas para protegerse de las consecuencias del incidente.
El/la Responsable de tratamiento y/o DPD serán los encargados de notificar a los/las afectados/as el incidente, debiendo comunicarlo a los mismos en un tiempo prudencial.
La notificación se realizará mediante email, SMS, correo postal o por teléfono e incluirá la siguiente información:

1. Datos de contacto de DPD, o en su caso, del punto de contacto en el que pueda obtenerse más información.
2. Descripción general del incidente y momento en que se ha producido.
3. Las posibles consecuencias de la brecha de la seguridad de los datos personales.
4. Descripción de los datos e información personal afectados/as.
5. Resumen de las medidas implantadas para controlar los posibles daños.
6. Otras informaciones útiles a los afectados para proteger sus datos o prevenir posibles daños.

EXCEPCIONES: No será necesaria la notificación a la Autoridad de Control cuando el/la responsable pueda demostrar, de forma fehaciente, que la brecha de la seguridad de los datos personales no entraña un riesgo para los derechos y las libertades de las personas físicas.

Por ejemplo, si los datos ya se encontraban públicamente disponibles y su revelación no entraña ningún riesgo hacia el/la titular de los datos.

Asimismo, no será necesaria la comunicación a los/las afectados/as cuando:

- ✓ El/la responsable ha tomado medidas técnicas y organizativas adecuadas, como que los datos no sean inteligibles para personas o máquinas no autorizadas con anterioridad a la brecha de seguridad de datos personales (mediante el uso de: cifrados de datos de última generación, minimización, disociación de datos, acceso a entornos de prueba sin datos reales, etc.).

- ✓ Por ejemplo, es probable que no sea necesaria la notificación si se pierde un dispositivo móvil y los datos personales que contiene están cifrados. Sin embargo, sí que es posible que se requiera de notificación si esta fuera la única copia de los datos personales, o por ejemplo, la clave de cifrado en posesión del/de la responsable, estuviera comprometida.
- ✓ El/la responsable ha tomado con posterioridad a la brecha de seguridad de datos personales las medidas de protección que mitiguen total o parcialmente el posible impacto para los/las afectados/as y garanticen que ya no hay posibilidad de que el alto riesgo se materialice. Por ejemplo, mediante la identificación y puesta en marcha inmediatamente de las medidas contra la persona que ha accedido a los datos personales antes de que pudieran hacer algo con ellos.
- ✓ Cuando la notificación a los/las afectados/as suponga un esfuerzo desproporcionado a nivel técnico y organizativo. Por ejemplo, cuando los detalles de contacto se hayan perdido como resultado de la brecha, o aquellos casos en los que se tenga que desarrollar un nuevo sistema o proceso para realizar la notificación, o se requiera la dedicación excesiva de recursos internos para la identificación de los/las afectados/as. Ante esta situación, se realizará la notificación de manera pública a través de los canales establecidos por el/la responsable.

ÍNDICE

FORMATO DE GESTIÓN DE INCIDENCIAS

MODELO DE COMUNICACIÓN DE INCIDENCIA EN EL TRATAMIENTO DE LA INFORMACIÓN

ENTIDAD RESPONSABLE:
Fundación para la Investigación de Málaga en Biomedicina y Salud -FIMABIS-
Instituto de Investigación Biomédica de Málaga y Plataforma en Nanomedicina -IBIMA Plataforma BIONAND-
C.I.F.: G29830643
Parque Tecnológico de Andalucía (PTA)Avenida Severo Ochoa, 35, 29590, Málaga.
tlf. 951 440 260- 951 440 263; fimabis@fimabis.org / ibima@ibima.eu

Delegado Protección de Datos: José Montilla Chicano, DPD_ProteccionDatos@ibima.eu

ENTRADA:…….. DÍA:…… MES:…… AÑO:…… HORA:……

IDENTIFICACIÓN DEL PERSONAL QUE REALIZA LA COMUNICACIÓN:
Nombre y Apellidos:
DNI/NIE:
Cargo:

1. COMUNICACIÓN DE INCIDENCIA

1.1.-Descripción de la incidencia producida:
_____
_____
_____

1.2.- Describir las consecuencias probables en la seguridad de los datos personales (en caso de conocerse):
_____
_____
_____

2. RELACIÓN DE DOCUMENTACIÓN ADJUNTADA:

1.-……..
2.-……..
3.-……..

3. OTROS COMENTARIOS

Fecha envío comunicación	Firma comunicador/a:
Fecha de recepción	Firma Responsable y DPD

ÍNDICE

ANEXO C.- PROTOCOLO DE GESTIÓN DE CORREO CORPORATIVO

INTRODUCCIÓN

El correo electrónico corporativo o institucional es un recurso proporcionado por **FIMABIS,** con el fin de facilitar la comunicación del personal vinculado a la entidad, ya sea para comunicación interna o externa.
En la presenta guía se recogen las directrices que se han de tener en cuenta para un buen uso y seguridad del correo electrónico corporativo.
Este documento y las normas que incluyen se deberá hacer extensible a la totalidad del personal de administración y servicios, así como a personal investigador o docente vinculado y que dispongan de una cuenta de correo corporativo, pues es responsabilidad de cada usuario de correo electrónico conocer y aplicar las recomendaciones desarrolladas en esta política de uso.

Recuerden que tiene a su disposición para cualquier consulta, duda o sugerencia:

- ✓ Unidad de Sistemas de la Información
- ✓ Delegado de Protección de Datos

Alcance

Hay que considerar, que, en el desarrollo de las actividades y funciones de la Entidad, el uso del correo electrónico tiene un impacto directo tanto en términos de tecnología, como de procesos y personas. En base a esta premisa, se enumeran los objetivos generales que se pretenden alcanzar con la elaboración de esta política de uso:

- Tecnología: Establecer y revisar que se toman las medidas técnicas oportunas para garantizar la seguridad en cuanto al uso del correo electrónico institucional.

- Procesos: Disponer de una política interna de uso del correo institucional que sea lícita, segura y sirva para prevenir e impedir errores o incidentes de carácter operativo, técnico o legal y que redunde en la mejora de la actividad, como siempre, orientado a la excelencia y la responsabilidad proactiva.

- Personas:
  - Comprobar que todo el personal conoce las recomendaciones de uso, así como los riesgos de un mal uso del correo electrónico.
  - Identificar las buenas prácticas en el uso del correo electrónico que redundarán en una optimización de tiempos y recursos.
  - Detectar posibles consecuencias de un uso inapropiado del correo electrónico como medida de prevención.

Disposiciones generales

El/la usuario/a tiene que hacer un buen uso del correo electrónico que le ha sido atribuido para el ejercicio de sus funciones y es responsable de los recursos que tiene asignados y de todas las acciones que se lleven a cabo en su utilización. Con este objetivo, tiene que cumplir las normas descritas en este documento.

Las presentes directrices son extensibles a las personas usuarias que tengan atribuida la gestión de cuentas de correo tanto genéricas (contabilidad@fimabis.org - @ibima….), como particulares Crisostomogutierrez@fimabis.eu). Si bien se reseña el dominio @fimabis.org, se deben considerar incluidos todos los dominios corporativos que la Entidad determine y ponga en uso.

- ✓ Todo personal de administración y servicios, así como investigadores y colaboradores están obligados a utilizar la cuenta de correo que le proporciona la Entidad para comunicarse, en lo que al desempeño de su trabajo o cuestiones relacionadas con la institución se refiere. De igual modo, no se permite la utilización de cuentas de correo personales (salvo necesidad) para la comunicación referente o vinculada, al desarrollo de las funciones y trabajo, propias de la Entidad. No obstante, se podrán usar aquellas pertenecientes a entidades o corporaciones relacionadas (UMA, SAS, etc)
- ✓ Los/las usuarios/as asumen la responsabilidad del uso que hacen de sus cuentas de correo electrónico institucionales, siendo conscientes de que cualquier mensaje que lleve el dominio **@fimabis…, @ibima….** representativa de la Entidad en su conjunto.
- ✓ Está prohibido facilitar u ofrecer el uso de la cuenta de correo electrónico (usuario/clave de acceso al servicio) a terceras personas.
- ✓ No se permite usar la cuenta de correo electrónico para actividades privadas, es decir, para actividades no relacionadas con **FIMABIS-IBIMA** y del trabajo o actividad propia de las funciones encomendadas.
- ✓ Está prohibido difundir información confidencial o revelar información que desacredite o pueda perjudicar la reputación de la Entidad, comprometa la reputación de nuestra organización o viole la legislación vigente, tanto autonómica, nacional o europea.
- ✓ Los mensajes han de ir firmados de tal forma que identifique a la Entidad y la vinculación del/la usuario/a con la misma.
- ✓ Los mensajes internos han de dirigirse exclusivamente a las personas involucradas e interesadas en el asunto, sin incluir largas e inútiles cadenas de receptores.
- ✓ Hay que evitar la dispersión de la información a largas cadenas de destinatarios/as o copiados, tratando de ceñirse a aquellas personas que realmente deben opinar y decidir en el asunto en cuestión.
- ✓ No deben arrastrase cadenas de mensajes previos trasladando la información a destinatarios/as que podrían no estar indicados en la interlocución inicialmente originada, pudiendo en muchos casos atentar contra la intimidad de información de los/las primeros/as remitentes.
- ✓ El correo electrónico es una herramienta para el intercambio de información entre personas, no se permite su uso como herramienta de difusión masiva e indiscriminada de información.
- ✓ No está permitido utilizar el correo electrónico con fines comerciales o financieros. No se permite el uso del correo electrónico facilitado para contratar servicios personales no relacionados con la actividad profesional.
- ✓ No se debe participar en la propagación de cartas encadenadas, participar en esquemas piramidales o similares.
- ✓ Si los/las destinatarios/as solicitan que se detenga el envío de correos electrónicos por parte de la Entidad, se deberá comunicar al responsable del departamento y DPD, debiendo abstenerse de ningún otro envío.
- ✓ Si la Entidad recibiera quejas, denuncias o reclamaciones por mala praxis en este ámbito, se podrán tomar las medidas sancionadoras adecuadas en base a lo establecido por el **Estatuto de los Trabajadores, así como normativa conexa**, aparte de las posibles responsabilidades, administrativas y/o penales, del personal implicado.
- ✓ Las cuentas de correo de la Entidad pueden ser auditadas para comprobar el uso de correcto de las mismas, siempre respetando las directrices legales de protección de datos y secreto de las comunicaciones.
- ✓ Si, en el ejercicio de sus funciones, el personal informático detecta cualquier anomalía que muestre indicios de usos ilícitos, lo pondrá en conocimiento del Responsable de la Entidad y, si procede, deshabilitará el servicio.

ÍNDICE

- ✓ Para asegurar un normal funcionamiento del servicio y un uso eficiente de los recursos del sistema de correo, el/la usuario/a se compromete a leer periódicamente su correo y a avisar de cualquier incidencia que pueda surgir y que estime puede afectar al normal comportamiento del servicio.
- ✓ Cuando la Entidad detecte que la persona trabajadora hace un mal uso del correo electrónico que se le ha asignado, se lo advertirá formalmente por escrito, sin perjuicio de la aplicación, si procede, del régimen disciplinario correspondiente.

CUESTIONES LEGALES: Protección de Datos de Carácter Personal

La dirección de correo electrónico asociada a una persona física se considera un dato de carácter personal, por lo que su tratamiento deberá respetar lo estipulado en el Reglamento General de Protección de Datos (RGPD) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD 3/2018). No obstante, se reseña lo expuesto por el RGPD 2016/679 en su Considerando 14: (*14) La protección otorgada por el presente Reglamento debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales. El presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto.*

En la medida en que la publicación de la dirección de correo electrónico laboral o profesional sea necesaria como parte del desarrollo de las funciones que puede tener atribuidas un determinado puesto de trabajo, su difusión debe considerarse amparada en el artículo 6.1 b) del RGPD. De igual manera, el artículo 19 de la LOPDGDD habilita el tratamiento de los datos de contacto (como es el correo electrónico profesional) fundamentando dicho tratamiento en el interés legítimo de la entidad (artículo 6.1. f) del RGPD) siempre que se cumplan los siguientes requisitos:

- ✓ Que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional.
- ✓ Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios.

Siempre es recomendable limitar la difusión de la dirección electrónica de los/las usuarios/as a aquellos supuestos en que resulte necesario para las funciones atribuidas a cada una de ellas. En el resto de supuestos, publicar la dirección de correo electrónico **solamente bajo comunicación interna**. Además, se debe incorporar, en el lugar donde se difundan las direcciones, un recordatorio de los usos admitidos de estas direcciones.

También es preciso incorporar mecanismos para evitar la indexación de las direcciones de correo, cuando se publiquen en la web, para evitar que se puedan utilizar para envíos masivos de correos electrónicos.

Es imprescindible no ceder a terceras personas las direcciones de correo que forman parte del directorio corporativo para finalidades diferentes de aquellas que resulten necesarias para desarrollar las funciones encomendadas a la Entidad.

ÍNDICE

GESTIÓN DEL BUZÓN DE CORREO

Se recuerda que, la normativa de protección de datos establece que los datos de carácter personal deben ser cancelados por la Entidad (Responsable del Tratamiento) cuando ya no sean necesarios en relación con los fines para los que fueron recogidos.

Cada usuario/a es responsable de realizar copias de los mensajes de correo electrónico si considera de relevancia o importancia para la compañía, y descargarla en su carpeta local. El servicio de Correo no es un dispositivo de almacenamiento masivo o permanente. Es responsabilidad del/la usuario/a limpiar su cuenta de correo periódicamente por seguridad ante acceso no autorizados y para que exista espacio disponible.

Corresponde a cada usuario/a velar para que la gestión de la información contenida en su correo electrónico sea adecuada. No obstante, se apuntan algunas normas que pueden ayudar a su correcta gestión:

- ✓ Hay que revisar y vaciar periódicamente la bandeja de entrada y, si procede, la de salida. Se recomienda que estas acciones se realicen, como mínimo, una vez cada 30 días.
- ✓ Hay que eliminar los mensajes que no se tengan que conservar y archivar el resto de mensajes en la carpeta o subcarpeta adecuada. Para su conservación a largo plazo es necesario migrarlos a un formato abierto o estándar, como .txt, .pdf o preferentemente .xml.
- ✓ Hay que borrar también, periódicamente, los mensajes de la papelera o carpeta de eliminados.
- ✓ Uso de las direcciones publicadas en la Intranet de la Entidad
- ✓ Las direcciones de los correos electrónicos del personal al servicio de la Entidad se podrán publicar en la intranet corporativa. Estas direcciones se pueden utilizar para las comunicaciones entre el personal vinculadas al ejercicio de las funciones respectivas.

MEDIDAS DE SEGURIDAD

Las personas usuarias de correo electrónico tienen que cumplir las medidas de seguridad siguientes:

- ✓ Guardar el usuario y la contraseña de acceso a la cuenta de correo de forma segura y no facilitarlos a otras personas, ni siquiera a efectos de mantenimiento del sistema.
- ✓ No utilizar una contraseña fácilmente deducible. La contraseña deberá tener una complejidad mínima de ocho caracteres alfanuméricos.
- ✓ No hacer uso de la opción de guardar la contraseña que se ofrece al/la usuario/a para evitar reintroducirla en cada conexión.
- ✓ Bloquear el acceso a la cuenta de correo, en caso de ausentarse del puesto de trabajo durante la jornada.
- ✓ No seguir cadenas de mensajes.
- ✓ No desactivar los filtros de correo y las opciones de seguridad activadas por el administrador del sistema.
- ✓ No abrir mensajes sospechosos. Comunicando cualquier sospecha a la Unidad de Sistemas de la Información de forma inmediata.
- ✓ No enviar, reenviar o responder mensajes de correo que contengan datos sensibles (Datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, así como el tratamiento de datos relativos a la salud, vida sexual o la orientación sexual de una persona física), sin la autorización de los Responsables de Seguridad de la Entidad, salvo que se haya autorizado previamente.
- ✓ En caso de detectar una incidencia durante el uso del correo electrónico, la persona afectada lo deberá que poner en conocimiento de la Unidad de Sistemas de la Información de forma inmediata.

- ✓ Situad y orientad las pantallas de los terminales de manera que se preserve el contenido de los mensajes respecto de terceras personas que se puedan encontrar en las dependencias donde se encuentra el puesto de trabajo.
- ✓ No se debe instalar software no autorizado por la empresa.
- ✓ Se recomienda que no esté activada la opción de vista previa en los correos.

ÍNDICE

AUSENCIA DE LA PERSONA TRABAJADORA Y/O DESTINATARIO/A

En caso de ausencia prolongada, se debe activar un mensaje de imposibilidad de lectura para facilitar otra dirección de contacto que garantice la continuidad de la actividad.

Para activar el mensaje de ausencia de oficina en Outlook, debemos ir a "Archivo" y seleccionar "Respuestas automáticas (Fuera de oficina)". El texto del mensaje de ausencia de oficina podrá ser, por ejemplo, como el que sigue:

"Muchas gracias por su email. No puedo atender a su correo, por favor póngase en contacto con ***…….@fimabis…. , @ibima…… .*** *Un cordial saludo."*

CESE DE LA RELACIÓN LABORAL

La Entidad puede cancelar la prestación del servicio de correo en el momento en que finalice la relación contractual o vinculante con la misma, o cuando el/la usuario/a esté haciendo un mal uso de él. Los mensajes recibidos en la cuenta corporativa, podrán ser analizados para determinar si resultan necesarios para la continuidad de la actividad o bien si se pueden suprimir.

En cualquier caso, antes de que el/la usuario/a cese su relación con la Entidad, se le debe dar la posibilidad de borrar todos los mensajes de carácter privado que considere oportunos. Si bien se recuerda que no está autorizado el uso de cuentas corporativas con finalidades privadas, no obstante, aún siendo una infracción el uso privado, no se puede acceder al mismo.

Se debe bloquear la cuenta lo más tarde posible en el último día de vinculación con la Entidad, es decir, no se le debe prohibir el acceso a su cuenta antes de la terminación de dicha vinculación, ya sea laboral o colaboradora. Además, el/la usuario/a debe ser informado/a del bloqueo de su cuenta. En ese mismo último momento, se deberá activar un mensaje automático de respuesta que informe a cualquier persona que envíe un email de que la persona en cuestión ya no trabaja en la Entidad o no está vinculada a ella, proporcionar la fecha desde la que la cuenta ha sido bloqueada y datos de contacto alternativos de la persona durante un periodo razonable de tiempo.

No obstante, de recibirse algún correo que pueda considerarse de carácter privado, se deberá contactar con el/la usuario/a cancelada, o bien con el/la remitente, a fin de que tomen las acciones oportunas sobre dicho correo. No se podrá abrir el contenido de dicho correo

Entre un mes y tres meses después del cese de la relación con la Entidad, la cuenta debe ser borrada y la respuesta automática desactivada.

Las cuentas corporativas vinculadas a departamentos u órganos de gestión o administrativos (contabilidad@fimabis...., o @ibima….) serán redireccionadas al personal que el Responsable designe.

Se señala que la Sala de lo Penal del Tribunal Supremo, en su sentencia 2844/2014, determina que aquellos correos electrónicos que no hayan sido abiertos por el titular de la cuenta están sujetos al secreto de las comunicaciones (artículo 18.3 de la Constitución Española), no así respecto de aquellos correos electrónicos ya leídos o abiertos, para los cuales efectivamente, rige lo establecido por la Sala de lo Social (Sentencia de 26/09/ 2007, la Sección 1ª de la Sala de lo Social de dicho tribunal, dictada

ÍNDICE

en unificación de doctrina, reconoce que el control por parte de la empresa de los medios informáticos puestos a disposición de un trabajador, vendrían amparados por el citado artículo 20.3. del Estatuto de los Trabajadores), es decir, podrán monitorizarse y controlar su contenido siempre y cuando se haya prohibido el uso de los mismos para cuestiones personales y se haya informado de la posibilidad de monitorización y control a través de la normativa interna en la empresa.

ACCESO A LA CUENTA DE CORREO ELECTRÓNICO POR PARTE DE LA ENTIDAD

Tanto el correo electrónico como la navegación por internet son medios de la Entidad, y por tanto su utilización debe ser únicamente laboral y profesional, quedando dentro del ámbito del poder de control del empresario, establecido en el art. 20.3 del Estatuto de los Trabajadores. Dicho control obedecerá a comprobar la corrección en el uso de estos medios informáticos, para corroborar si se está cumpliendo con el deber o prestación laboral y/o profesional, así como si su uso se ajusta a las finalidades que lo justifican, o por razones de seguridad, prevención de infracciones penales.

Por ello cualquier información obtenida por este medio podrá ser utilizada con fines disciplinarios. No obstante, deberá superar, un juicio de proporcionalidad, es decir, que la medida sea susceptible de conseguir el objetivo propuesto (juicio de idoneidad), que no exista otra medida más moderada para la consecución de tal propósito (juicio de necesidad) y finalmente, que la misma sea proporcional de acuerdo con los bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)

La Entidad solo puede acceder a las cuentas de correo electrónico corporativo facilitadas cuando el acceso esté justificado y no haya ningún otro mecanismo que permita alcanzar el objetivo perseguido sin necesidad de acceder a las mismas. El medio y el alcance del control tienen que ser proporcionados a la finalidad que se persiga.

Así, se debe limitar el acceso a los datos sobre el/la emisor/a y el/la receptor/a, la hora de la comunicación y otros datos como el número de mensajes enviados, el volumen de información o el tipo de archivos que se haya adjuntado u otros sistemas de análisis automatizado de los mensajes entrantes y salientes que no analicen su contenido. Solo si esta información no es suficiente para alcanzar la finalidad perseguida se podrá acceder al contenido de los mensajes, siempre que se cumplan las garantías apropiadas, evitando entrar en los mensajes que se puedan identificar como privados. En caso de que un mensaje de esta naturaleza se abra por error, hay que cerrarlo tan pronto como se pueda constatar su naturaleza privada, y comunicarlo al Responsable y al/la interesado/a, si bien se recuerda la prohibición de usar el correo electrónico con fines privados y personales.

El acceso que se lleve a cabo en cualquiera de los supuestos descritos tiene que quedar debidamente reflejado en el registro de incidencias y se tiene que limitar a la información que resulte indispensable para alcanzar alguno de los objetivos siguientes:

➢ Acceso para realizar tareas de mantenimiento del correo electrónico

El acceso a las cuentas de correo electrónico corporativo para las tareas de mantenimiento, el soporte técnico o la seguridad del sistema no tiene que comportar el acceso al contenido de los mensajes.

➢ Acceso para garantizar la continuidad de la actividad laboral

Para garantizar la continuidad funcional de la actividad, en caso de ausencia imprevista de la persona receptora (vacaciones, enfermedad, etc.). Si, por una necesidad improrrogable ligada a la actividad vinculada a la Entidad, hay que acceder al contenido de los mensajes del correo electrónico de la persona ausente, ésta puede delegar en otra persona para que verifique la forma en que se lleva a cabo el acceso, siempre bajo autorización expresa y documentada.

Si ello no es posible, hay que tener en cuenta:

- ✓ El responsable del departamento u órgano superior de la persona ausente tiene que valorar de forma motivada la necesidad de la intervención para la continuidad del servicio.
- ✓ El acceso a la cuenta de correo electrónico se tiene que comunicar a la persona ausente con suficiente antelación. Si no fuera posible esta comunicación previa, se tiene que hacer posteriormente, tan pronto como sea posible.
- ✓ Se debe acceder a ella bajo la supervisión del responsable del departamento u órgano superior de la persona ausente y, en el caso de que se le haya podido comunicar, con su asistencia o la de la persona que designe, si lo desea.

ÍNDICE

➢ Acceso cuando haya indicios de un posible mal uso

La Entidad puede hacer controles automatizados sobre el uso del correo electrónico, con el fin de velar por el normal funcionamiento del sistema (volumen de tráfico, volumen de los mensajes enviados, etc.).

La Entidad podrá acceder al contenido de los correos para comprobar, en el seno de una información reservada o de un procedimiento disciplinario, el uso del correo electrónico en aquellos casos en que haya indicios de que la persona usuaria ha hecho un mal uso de él.

En este sentido, para el desempeño de las funciones y actividad de los/las usuarios/as, se pueden poner a su disposición medios tecnológicos que son titularidad de la entidad (ordenador, correo electrónico, acceso a Internet, etc.). El uso de dichos medios queda limitado al desempeño de las tareas que la persona tenga asignadas, no estando permitidos usos privados. Con el fin de garantizar el cumplimiento de sus obligaciones y los compromisos asumidos, la entidad podrá controlar o supervisar el uso que haga el/la usuario/a de los medios indicados y acceder a ellos, quedando el trabajador informado de ello.

Si hay indicios de un mal uso del correo, por incumplir las normas que haya aprobado la Entidad, se tiene que poner en conocimiento de la persona interesada, a menos que esto pueda obstaculizar las investigaciones que procedan. Cuando este mal uso pueda ser constitutivo de delito o falta, se ha de comunicar al ministerio fiscal.

Cualquiera de estos casos puede dar lugar a una información reservada o a un procedimiento disciplinario, en cuyo seno se pueden adoptar las medidas que estén al alcance para solucionar el problema, que pueden incluir el bloqueo de los mensajes. En este acceso, que tiene que ser proporcionado al tipo de riesgo que se pueda derivar del mal uso del correo para la Entidad o terceras personas, conviene tener en cuenta:

- ➢ El acceso lo tiene que llevar a cabo la persona designada por el Responsable de la Entidad, en presencia de la persona interesada, si es posible, y de testigos que puedan dar fe del acceso realizado.
- ➢ Una vez se ha accedido, se elaborará un informe de las actuaciones realizadas y de los resultados obtenidos e incorporarlo, si procede, al expediente correspondiente.

ÍNDICE

FIRMA DEL CORREO CORPORATIVO

Es muy importante tener en cuenta que la firma incluida en el correo electrónico es un elemento clave de la marca institucional, que contribuye a la percepción sobre nuestra institución.

Por ello, se establece, a modo de ejemplo, un modelo genérico, como se muestra a continuación, para la firma de correo electrónico, con el objetivo de mantener la unidad gráfica entre todo el personal laboral o vinculado a la Entidad.

…(nombre y apellidos)
…(Unidad/cargo)……
Email: **……@ibima.eu** / @fimabis
Móvil: **+…**…… Corp: **…**……
Málaga TechPark; Parque Tecnológico de Andalucía (PTA)
C/ Severo Ochoa, 35.
29590 Málaga (Málaga)

Antes de imprimir este mensaje valore si verdaderamente es necesario. De esta forma contribuimos a la preservación del Medio Ambiente.

La información incluida en el presente correo electrónico es CONFIDENCIAL, siendo para el uso exclusivo del destinatario arriba mencionado. Si usted lee este mensaje y no es el destinatario señalado, o el empleado responsable de entregar el mensaje al destinatario, o ha recibido esta comunicación por error, le informamos que está totalmente prohibida cualquier divulgación, distribución o reproducción de esta comunicación y le rogamos que nos lo notifique y borre el mensaje. La responsabilidad de su verificación es suya exclusivamente. Las opiniones expresadas en este e-mail pertenecen a la persona que lo envía y no necesariamente a la Empresa. Gracias.

En cumplimiento de la normativa de protección de datos, le informamos de que el tratamiento de sus datos personales forma parte del Registro de Actividades de Tratamiento de FIMABIS. Usted puede consultar el listado de actividades de tratamiento en el siguiente enlace: http://www.fimabis.org/wp-content/uploads/2021/04/RAT-_FIMABIS.xlsx

RECOMENDACIONES PARA EL USO ADECUADO DEL CORREO INSTITUCIONAL

Se presentan, para ampliar recomendaciones, las formuladas por el Instituto Nacional de Ciberseguridad (www.incibe.es).

Tecnología. Las recomendaciones de uso del correo electrónico tienen un impacto directo en la tecnología utilizada. Es por ello que resulta básico comenzar por este punto, para garantizar la seguridad en sucesivos aspectos. En términos de tecnología y teniendo en cuenta las características de la Entidad, estas serían las sugerencias de uso del correo electrónico institucional:

- ✓ Auditoría periódica e instalación de actualizaciones, a fin de identificar el estado de los programas y aplicaciones, y garantizar que estamos gozando siempre de la máxima seguridad posible o aplicar mejoras de ser necesario, como puede ser incluir nuevas funcionalidades, solventar fallos o resolver vulnerabilidades de seguridad.
- ✓ Instalar y activar aplicaciones anti-malware y filtros anti-spam en el servidor.
- ✓ Instalar una tecnología de cifrado y firma digital que se pueda usar con el correo electrónico para proteger la información confidencial y asegurar la autenticidad de la Entidad como remitente.
- ✓ No publicar las direcciones de correo corporativas en páginas web ni en redes sociales sin utilizar técnicas de ofuscación o enmascaramiento, para que estas no puedan ser captadas para ser incluidas en listas de envío de spam. Por ejemplo, en vez de disponer nombre y cuenta de correo y/o teléfono en formato texto, emplear formato imagen

ÍNDICE

Procesos. Resulta fundamental que, en base a las premisas técnicas, se articulen los mecanismos y procesos oportunos para que las personas puedan realizar un uso adecuado de los recursos. Así, en términos de procesos institucionales, es importante considerar las siguientes recomendaciones:

- ✓ Disponer de una normativa referente al uso del correo electrónico, como puede ser esta política de uso del correo electrónico, que el usuario/a aceptará junto a su cuenta de correo.
- ✓ Concienciación y formación, pues nada más importante que conocer los riesgos para poder evitarlos.
- ✓ Garantizar y revisar el cumplimiento legal de la normativa institucional.

Personas. Una vez se encuentren cubiertas las recomendaciones anteriores, en términos técnicos y de procesos, corresponderá a las personas cumplir con las recomendaciones que a continuación se enumeran, por su impacto en su día a día, existiendo una dependencia directa de ellos para garantizar su cumplimiento, a fin de contribuir al buen uso del recurso:

- ✓ Nunca usar el correo corporativo con fines personales.
- ✓ Asegurarse de que el contenido del correo cumple las normas marcadas por la Entidad.
- ✓ Usar una contraseña segura y no compartirla con terceros.
- ✓ Identificar a los/las remitentes de correo electrónico y, de tener dudas sobre si su identidad ha sido suplantada, contactar con la persona por otra vía antes de abrir el correo, descargar archivos adjuntos o dar información confidencial. Es recomendable analizar las extensiones, tanto de dominio como de formato de documentos (por ejemplo, sería sospechoso: ….@hprts.1234.br, o un adjunto con formatos ejecutables tipo exe., src,. u otros que resulten igualmente sospechosos)
- ✓ Analizar los enlaces incluidos en correos antes de acceder a ellos, revisando si el texto de la URL se corresponde con el hipervínculo.
- ✓ No responder a correos spam o basura. Se recomienda agregar al remitente a la lista de spam y eliminarlo.
- ✓ Ser consciente de técnicas como el phishing o las campañas de envío de correos fraudulentos a fin de identificarlos.
- ✓ Utilizar la copia oculta (CCO) a fin de proteger la privacidad de los destinatarios siempre que se envíe un correo a varias personas.
- ✓ Evitar el reenvío de correos electrónicos sin permiso del/la emisor/a inicial. Todos los correos que se envíen en la organización podrán ser reenviados a otros miembros, siempre que la motivación sea el desempeño de las funciones y que no se trate de información confidencial.
- ✓ No consultar el correo electrónico institucional en público o con conexiones públicas, pues el tráfico de datos puede ser interceptado por cualquier usuario/a próximo o de esta red.
- ✓ Bloquear o cerrar la sesión en el equipo de trabajo de necesitar ausentarse.

Mas información en https://www.incibe.es/protege-tu-empresa/kit-concienciacion

CONSECUENCIAS DEL USO INADECUADO DEL CORREO INSTITUCIONAL

En esta sección se señalan los riesgos a los que se puede exponer una entidad por no seguir dichas recomendaciones y por el uso inapropiado del correo electrónico:

- ➢ Ataques informáticos.
- ➢ Compromiso de las redes, sistemas de información e información de carácter confidencial.
- ➢ Riesgos de índole jurídica a nivel nacional o internacional como consecuencia de una inadecuada comunicación.
- ➢ Incumplimiento de la normativa en materia de protección de datos por divulgar o comunicar datos de terceros sin su consentimiento.
- ➢ Crisis de reputación institucional asociadas a un mal uso del recurso.
- ➢ Pérdida de operatividad, tiempo y recursos de personal y servicios.
- ➢ Repercusiones administrativas y/o penales ante incumplimiento legal

ÍNDICE

BUENAS PRÁCTICAS EN EL USO DEL CORREO ELECTRÓNICO

Según todo lo expuesto anteriormente, se establecen las siguientes buenas prácticas para el uso del correo electrónico en **FIMABIS-IBIMA**.

Optimización del uso

- ✓ Es imprescindible separar el uso profesional del uso personal en las cuentas de correo electrónico. La cuenta de correo institucional que la Entidad proporciona es una cuenta de carácter profesional y no es equivalente a una cuenta personal ya que está asociada a la organización.
- ✓ Conviene conocer las herramientas y recursos disponibles en la Entidad y usar cada una para la finalidad con la que fue diseñada. Por ejemplo, el correo electrónico no es el mecanismo más adecuado ni eficiente para transferir ficheros, es más adecuado el uso de conexiones internas (VPN) o en todo caso de unidades extraíbles. Si no queda más remedio que hacerlo por email es mejor utilizar el formato zip y bajo contraseña.
- ✓ Antes de contestar un correo que se ha enviado a diferentes personas, hay que valorar la necesidad de enviar la respuesta solo al/la remitente o también al resto de las personas puestas en copia.
- ✓ Se debe respetar la privacidad de los mensajes y el/la destinatario/a. Solo se debe utilizar la opción de reenviar en aquellos casos en que tanto el/la emisor como el contenido del mensaje, y toda la información de la cadena de correos que forman parte de él, puedan ser accesibles para la persona destinataria. No obstante, es preferible evitar el envío de mensajes en cadena para evitar dar a conocer indebidamente contenidos a terceras personas o incluso, para evitar la propagación de virus o software malicioso.
- ✓ Es preferible utilizar las cuentas de correo genéricas de los departamentos, sobre todo si no se está seguro sobre a quién es preciso dirigirse. También es de utilidad incluirlo en la copia del mensaje.

En alguna ocasión puede llegar por error un email, en cualquier caso, no es conveniente ignorarlo. Lo preferible es contactar con el/la remitente e indicarle el error, remitirlo a la persona de interés o trasladar la información necesaria para su sol

ANEXO D. PROTOCOLO GESTIÓN DE CURRICULUMS

PREÁMBULO

La legislación vigente en materia de protección de datos (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y Reglamento Europeo 2016/679) tienen como finalidad proteger la intimidad y privacidad de los individuos, salvaguardar sus derechos, y esto es algo que concierne directamente a las relaciones laborales.

Esta normativa considera como datos personales toda aquella información que permita identificar a una persona, ya sean estos datos escritos, de vídeo o audio. Estableciendo normas y prácticas que se deben de cumplir a la hora de tratar y transmitir datos personales, siendo importante destacar que no consiste solo en un cumplimiento legal, si no, que responde a la necesidad de salvaguarda de los derechos de las personas.

Se señala la vinculación en la función pública de la entidad, lo cual le hace susceptible del cumplimiento de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, así como su adecuación al Esquema Nacional de Seguridad

Expuesto lo anterior, unos de los tratamientos que se dan en las empresas/entidades es el de los curriculum vitae (CV), de demandantes o postulantes/solicitantes de empleo, el cual exige unas medidas de licitud y seguridad bien definidas. Más aún, teniendo en cuenta que se comunican/ceden gran variedad de datos de carácter personal.

En la recepción/envío de CV, si bien se suele partir de una "autorización" tácita por parte del/ de la interesado/a, hay que tener en cuenta que la comunicación voluntaria, e incluso espontánea, de datos por parte de solicitantes de trabajo, no exime, ni es óbice, para no implementar las medidas de seguridad y respeto a los derechos de las personas.

Siendo así, el presente protocolo pretende determinar las obligaciones, pautas y formas del tratamiento de CV en la empresa/entidad.

DISPOSICIONES GENERALES

I.- PRINCIPIOS del Tratamiento de la información

RGPD. Artículo 5 Principios relativos al tratamiento
1.Los datos personales serán:
a) tratados de manera lícita, leal y transparente en relación con el interesado ***(«licitud, lealtad y transparencia»);***
b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales ***(«limitación de la finalidad»);***
c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados ***(«minimización de datos»);***

ÍNDICE

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan ***(«exactitud»);***
e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado ***(«limitación del plazo de conservación»)****;*
f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas ***(«integridad y confidencialidad»).***
2.El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo ***(«responsabilidad proactiva»).***

II.- DEBERES

II.1.- Licitud

El RGPD establece**:** Artículo 6 Licitud del tratamiento

1.*El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:*
a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

En el ámbito del tratamiento de CV se debe tener en especial consideración

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos; (si se ha recogido expresamente)

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

II.2.- Deber de información:

LOPDGDD 3/2018. CAP. I. Transparencia e información.
Art. 11. Transparencia e información al afectado.

La información se debe poner a disposición de los interesados en el momento en que se soliciten los datos, previamente a la recogida o registro, si es que los datos se obtienen directamente del interesado.

ÍNDICE

- En el caso de que los datos no se obtengan del propio interesado, por proceder de alguna cesión legítima, o de fuentes de acceso público, el Responsable informará a las personas interesadas dentro de un plazo razonable, pero en cualquier caso:
  - ✓ antes de un mes desde que se obtuvieron los datos personales,
  - ✓ antes o en la primera comunicación con el interesado,
  - ✓ antes de que los datos, en su caso, se hayan comunicado a otros destinatarios
- Esta obligación se debe cumplir sin necesidad de requerimiento alguno, y el responsable deberá poder acreditar con posterioridad que la obligación de informar ha sido satisfecha.

II.3.- Minimización:

El principio de "minimización de datos", viene definido por la AEPD como aplicar medidas técnicas y organizativas para garantizar que sean objeto de tratamiento los datos que únicamente sean precisos para cada uno de los fines específicos del tratamiento reduciendo, la extensión del tratamiento, limitando a lo necesario el plazo de conservación y su accesibilidad. Es decir, solo se podrán recoger los datos personales que se vayan a tratar; ni más ni menos, solo los que sean estrictamente necesarios. Además, solo podrán ser recogidos cuando vayan a ser tratados o bien mediante consentimiento de plazo de conservación.

En el ámbito del tratamiento de CV, hay que discriminar qué datos son realmente necesarios para un proceso de selección. Habitualmente se recogen:

- ✓ Nombre y apellidos
- ✓ DNI
- ✓ Fecha de nacimiento
- ✓ Domicilio
- ✓ Teléfono y correo electrónico
- ✓ Nacionalidad
- ✓ Estado civil
- ✓ Formación académica
- ✓ Experiencia laboral

No obstante, y en función del puesto ofertado, se podrían eludir algunas tipologías, que posteriormente y en base a la contratación se completarían, así, habría que considerar si es necesario para una preselección:

- ➢ DNI
- ➢ Fecha de nacimiento
- ➢ Nacionalidad
- ➢ Estado civil

Pudiéndose disponer tales campos como opcionales

II.3.1 Plazos de Conservación

La normativa de protección de datos establece la obligación de conservar los datos actualizados. Si bien, respecto al CV el RGPD no nos indica un plazo concreto para la conservación y actualización de datos, en la práctica se considera que, si un CV no se ha actualizado en 24 meses, se debe proceder a su bloqueo, para impedir su lectura, o su eliminación.

No obstante, se debe considerar obsoleto un CV no actualizado en 12 meses, y debe ser eliminado. Sin embargo, en aquellos casos en los que se constituya BOLSA DE TRABAJO, su periodo de conservación vendrá definido por las bases de la misma. Informándose de todos estos extremos a la persona solicitante

II.4.- Consentimiento

RGPD. Considerando (32) El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. (…) Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines.

42) Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento

En lo que respecta al CV el RGPD y la LOPDGDD nos dicen que, independientemente de la voluntariedad del interesado, es obligatorio recabar el consentimiento para el tratamiento de los datos personales de su CV.

Este consentimiento, además, debe ser, como ya se ha señalado, informado y expreso, es decir; se debe informar al interesado de:

- ✓ La existencia de un fichero con sus datos personales
- ✓ La finalidad del tratamiento para el cual se recogen sus datos
- ✓ La identidad del responsable del tratamiento
- ✓ La base jurídica del tratamiento
- ✓ La cesión de datos a terceros, incluidas transferencias internacionales (si se van a producir)
- ✓ Tiempo de conservación de los datos
- ✓ Dónde y cómo puede ejercer los derechos que la normativa dispone

II.5.- Seguridad

RGPD. Art. 5. (…) f) (los datos serán) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

La AEPD refiere la responsabilidad proactiva, la protección de datos desde el diseño, que exige a los responsables establecer las medidas técnicas y organizativas necesarias a lo largo de todo el ciclo de vida del tratamiento, tanto desde el momento inicial en que se lleva a cabo la definición del tratamiento y se determinan los medios como durante su puesta en marcha y funcionamiento habitual. Estas medidas y garantías deben establecerse atendiendo a la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como a los riesgos para los derechos y libertades de los interesados que pueda llegar a representar.

La protección de datos desde el diseño tiene por objetivo aplicar los principios de protección de datos en los procesos de diseño de los sistemas y procedimientos de la organización sobre los que se apoya el tratamiento de los datos, con un fin eminentemente preventivo y orientado tanto a evitar posibles daños a las personas físicas como, de manera colateral, los perjuicios que para la organización podría suponer la modificación o el rediseño de los sistemas en los que se llevan a cabo los tratamientos, una vez desarrollados e implantados, como consecuencia de la identificación de errores de diseño que pudieran suponer daños o perjuicios a los interesados y a sus derechos y libertades.

III.- METODOLOGÍAS

III.1.- Metodología de prestación de información:

Para hacer compatible la mayor exigencia de información que introduce el RGPD y la concisión y comprensión en la forma de presentarla, se recomienda adoptar un modelo de información por capas o niveles.

Así:

- Presentar una información básica en un primer nivel, de forma resumida, en el mismo momento y en el mismo medio en que se recojan los datos,
- Remitir a la información adicional en un segundo nivel, donde se presentarán detalladamente el resto de las informaciones, en un medio más adecuado para su presentación, comprensión y, si se desea, archivo.

Esquema:

Epígrafe	Información básica (1ª capa, resumida)	Información adicional (2ª capa, detallada)
"Responsable" (del tratamiento)	Identidad del Responsable del Tratamiento	Datos de contacto del Responsable
		Identidad y datos de contacto del representante
		Datos de contacto del Delegado de Protección de Datos
"Finalidad" (del tratamiento)	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Decisiones automatizadas, perfiles y lógica aplicada
"Legitimación" (del tratamiento)	Base jurídica del tratamiento	Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo.
		Obligación o no de facilitar datos y consecuencias de no hacerlo
"Destinatarios" (de cesiones o transferencias)	Previsión o no de Cesiones	Destinatarios o categorías de destinatarios
	Previsión de Transferencias, o no, a terceros países	Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
"Derechos" (de las personas interesadas)	Referencia al ejercicio de derechos.	Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento
		Derecho a retirar el consentimiento prestado
		Derecho a reclamar ante la Autoridad de Control
"Procedencia" (de los datos)	Fuente de los datos (cuando no proceden del interesado)	Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público
		Categorías de datos que se traten

ÍNDICE

Información básica (primera capa)

• La forma de presentación preferente de esta primera capa es en forma de tabla, garantizando

que dicha información quede dentro del "campo de visión" del interesado, según sea el medio utilizado en la recogida de la información. Estando claramente identificada con un título tal como "Información básica sobre protección de datos"

Si, por restricciones del diseño, no fuese factible, debe incorporarse una nota o llamada en el campo de visión de la firma, informando sobre dónde se sitúa la tabla con la información sobre protección de datos.

Ejemplo: "antes de firmar/enviar la solicitud, debe leer la información básica sobre protección de datos que se presenta en (…el reverso, al pié, etc…)"

Ejemplo (1ª capa concretado a la entidad):

Responsable	**Fundación para la Investigación de Málaga en Biomedicina y Salud -FIMABIS-** **Instituto de Investigación Biomédica de Málaga y Plataforma en Nanomedicina** -IBIMA Plataforma BIONAND- Ins. Reg. Fundaciones Consejería Justicia y Administraciones Públicas Junta de Andalucía nº MA-606 C.I.F.: G29830643 Parque Tecnológico de Andalucía (PTA)Avenida Severo Ochoa, 35, 29590, Málaga. tlf. 951 440 260- 951 440 263; fimabis@fimabis.org / ibima@ibima.eu
DPD	**DPD_ProteccionDatos@ibima.eu**
Finalidad	Gestión de empleo. Convocatorias. Bolsa de trabajo
Legitimación	Ejecución de un contrato/solicitud Consentimiento interesado/a
Destinatarios	No se cederán datos a terceros, salvo obligación legal. Se señala que, en base a la legislación de transparencia, los procesos de selección pueden ser publicados en los medios de comunicación de la Entidad
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, dirigiéndose a la entidad, como se explica en la información adicional
Información adicional	Puede consultar Registro de actividades, y la información adicional y detallada sobre Protección de Datos en nuestra página web https://www.ibima.eu/aviso-legal/ www.fimabis.org

La forma de presentar la segunda capa, con el resto de información necesaria, ya no debe estar condicionada en cuanto a la extensión de la información. Así, se puede proporcionar:

Información adicional en papel:

- En el mismo formulario cumplimentado (por ejemplo, en el reverso)
- Como un anexo o separata que se entregue al interesado y que pueda conservar
- Como información expuesta, claramente visible, en carteles, paneles, trípticos, etc, de los cuales se pueda solicitar una copia manejable para conservar.

Información adicional electrónica

- En una página web específica, a la que se accede mediante un hipervínculo
- Como un documento disponible para su descarga desde una URL
- Como información anexa o adjunta a un mensaje electrónico dirigido al interesado Información adicional telefónica:Como una locución que se le ofrezca al interesado, como complemento o alternativa a una oferta de disponibilidad de información adicional accesible electrónicamente o remitida, por correo postal o electrónico.

ÍNDICE

III.2. Metodología de prestación de información y consentimiento

La normativa de protección de datos de carácter personal, determina que es necesario incluir una cláusula de protección de datos para el tratamiento de datos personales en el CV.

A través de esta cláusula se informa a los/las candidatos/as de todos los aspectos relacionados con el tratamiento de sus datos personales, es decir, cumple la función de informar a los/las candidatos/as antes de obtener su consentimiento (tal y como vimos en puntos anteriores).

Como el método de recepción de CV varía, la inclusión de esta cláusula difiere en función de cómo reciba la empresa los currículums de sus candidatos/as:

- El/la candidata/a se postula en una oferta publicada por la empresa en un **portal/aplicación** de empleo/contratación: En este caso, la propia empresa o la plataforma en la que se publica la oferta (que puede ser la propia de la entidad contratante), serán las encargadas de facilitar la cláusula informativa y de consentimiento correspondiente. Esto se puede realizar mediante enlace a la referida clausula y "check" de aceptación, o bien la disposición de formato descargable para su aceptación y envío junto al CV.
- El currículum es enviado por el/la candidata/a, a través de **correo electrónico**, por iniciativa propia: la postulación espontánea, aunque el candidato haya enviado su currículum por motu propio, es necesario enviar un acuse de recibo con su cláusula de información y consentimiento correspondiente. Algo que puede ser implementado en el correo como contestación automática.
- El currículum es enviado por el/la candidata/a, a través de **correo ordinario**, en este caso dado el coste, de trabajo y recursos, que puede suponer la contestación, se debe valorar su tratamiento, dándose dos opciones:
  - Contestación por correo ordinario, o electrónico si lo ha facilitado como medio de contacto, con cláusula informativa y de consentimiento, o bien
  - Informar en la web corporativa de que no serán recogidos ni tratados los CV remitidos por correo ordinario.
- El currículum es presentado **personalmente,** en este modo, se proporcionará formulario de información y consentimiento para su firma y adhesión al propio CV. No se deberán aceptar sobres cerrados
- **Entrevista Telefónica**: En una entrevista telefónica se deberá ofrecer la información básica como una locución clara y concisa, pero asegurando que el interlocutor haya comprendido la información suministrada, antes de proceder a la recogida de la información. De ser posible la conversación, previo aviso, será grabada

III.3. Metodología de implementación de seguridad

Teniendo en consideración previa, las medidas de seguridad derivadas de la responsabilidad proactiva, entre otras:

- ✓ Seguridad de sistemas, equipos y redes
- ✓ Seguridad en archivo documental
- ✓ Restricción de acceso autorizados
- ✓ Compromiso de confidencialidad
- ✓ Análisis de riesgos, valoración EIPD

En el tratamiento y gestión de CV, se debe tener en especial vigilancia en el archivo en aplicaciones de correo electrónico. Si bien dichas aplicaciones no son gestores de archivo, es muy común su uso con tal fin. Ello es algo que expone la información a accesos/secuestros/perdidas indeseadas.

Los CV (y demás correos electrónicos recibidos) se deben archivar en carpetas exprofeso, con seguridad y restricción de acceso, siendo eliminadas de las aplicaciones de correo electrónico, lo cual incluye la propia dirección electrónica del remitente, con el fin de que por error no se establezcan comunicaciones desde la agenda de contactos.

IV.1.- REGISTRO ACTIVIDADES GESTIÓN CURRICULUM

a) Responsable	**Fundación para la Investigación de Málaga en Biomedicina y Salud -FIMABIS-** **Instituto de Investigación Biomédica de Málaga y Plataforma en Nanomedicina -** IBIMA Plataforma BIONAND- Ins. Reg. Fundaciones Consejería Justicia y Administraciones Públicas Junta de Andalucía nº MA-606 C.I.F.: G29830643 Parque Tecnológico de Andalucía (PTA)Avenida Severo Ochoa, 35, 29590, Málaga. tlf. 951 440 260- 951 440 263; fimabis@fimabis.org / ibima@ibima.eu
b) Delegado de protección de datos	**DPD_ProteccionDatos@ibima.eu**
c) **Base jurídica**	**RGPD: 6.1** a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. b) Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales. **Legislación vinculada:** Real Decreto Legislativo 2/2015, Ley del Estatuto de los Trabajadores. Ley 19/2013, de transparencia, acceso a la información pública y buen gobierno.
d) **Fines del tratamiento**	Gestión de solicitudes de empleo, bolsa de trabajo y curriculum personales.
e) **Colectivo**	Personal Solicitante
f) **Categorías de Datos**	Nombre y apellidos, DNI/Documento identificativo. Datos de contacto: dirección, email y teléfono. Datos de características personales: estado civil, nacionalidad, fecha y lugar de nacimiento. Datos académicos y profesionales: Titulaciones, formación y experiencia profesional.
g) **Categoría destinatarios**	Sin cesiones previstas, salvo exigencia legal. Se señala que, en base a la legislación de transparencia, los procesos de selección pueden ser publicados en los medios de comunicación de la Entidad
h) **Transf. Internacional**	No están previstas transferencias internacionales de los datos.
i) **Plazo supresión**	Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. En todo caso 12 meses, de no mediar actualización o requerimiento de cancelación o supresión.
j) **Medidas de seguridad**	Las medidas de seguridad implantadas se corresponden con las previstas en el Reglamento Europeo 2016/679 de protección datos de carácter personal y L.O.P.D.G.D.D. 3/2018, y ENS Control de accesos y autorizaciones. Seguridad física infraestructuras y edificios Seguridad lógica de sistemas. Seguridad de redes Compromiso fehaciente de confidencialidad por parte del personal
k) Ejercicio de derechos	**Fundación para la Investigación de Málaga en Biomedicina y Salud -FIMABIS-** **Instituto de Investigación Biomédica de Málaga y Plataforma en Nanomedicina -** IBIMA Plataforma BIONAND- C.I.F.: G29830643 Parque Tecnológico de Andalucía (PTA)Avenida Severo Ochoa, 35, 29590, Málaga. tlf. 951 440 260- 951 440 263; fimabis@fimabis.org / ibima@ibima.eu Email DPD: DPD_ProteccionDatos@ibima.eu Solicitud de tutela ante la Agencia Española de Protección de Datos. www.aepd.es
l) Más información	https://www.ibima.eu/aviso-legal/ www.fimabis.org

ÍNDICE

IV.2.- CLAUSULAS INFORMATIVAS CURRICULUM VITAE

IV.2.i.-CARTA CONTESTACIÓN CURRÍCULUM VITAE, Correo electrónico

Agradeciendo su interés por nuestra entidad y compartir con nosotros su CV. Queremos poner a su disposición la información sobre el tratamiento de datos personales que realizamos, así como obtener su consentimiento para dicho tratamiento.

¿Quién es el responsable del tratamiento de tus datos personales?

Fundación para la Investigación de Málaga en Biomedicina y Salud -FIMABIS-
Instituto de Investigación Biomédica de Málaga y Plataforma en Nanomedicina -IBIMA Plataforma BIONAND-

Ins. Reg. Fundaciones Consejería Justicia y Administraciones Públicas Junta de Andalucía nº MA-606
C.I.F.: G29830643
Parque Tecnológico de Andalucía (PTA)Avenida Severo Ochoa, 35, 29590, Málaga.
tlf. 951 440 260- 951 440 263; fimabis@fimabis.org / ibima@ibima.eu
Email DPD: DPD_PROTECCIONDATOS@IBIMA.EU

¿Con qué finalidad tratamos tus datos personales?

En FIMABIS-IBIMA vamos a tratar sus datos con la siguiente finalidad:

• Valorar y gestionar su perfil como candidato en relación a los procesos de selección de personal que estamos llevando a cabo o podamos realizar en el futuro que puedan ajustarse a tu perfil profesional.

• Llevar a cabo las actuaciones necesarias para la gestión de los procesos de selección de FIMABIS-IBIMA, a través de comunicaciones electrónicas, contactos telefónicos, entrevistas y pruebas selectivas.

¿Cuál es la legitimación para el tratamiento de tus datos?

La base que legítima el tratamiento de tus datos personales es el consentimiento otorgado, bien al apuntarte a una de nuestras ofertas de empleo o bien al remitir voluntariamente tu candidatura espontánea. No obstante, si lo desea, puede retirar su consentimiento en cualquier momento, si bien ello haría que su candidatura no pudiera ser tenida en cuenta en nuestros procesos de selección. En su caso, la retirada de su consentimiento no afectará a la licitud de los tratamientos efectuados con anterioridad.

Si ha facilitado referencias de contactos, ¿cómo los vamos a utilizar?

En el caso de que facilitase referencias y datos de terceros (contactos profesionales), manifiesta contar con el consentimiento de los mismos y se comprometes a trasladarles la información relativa al tratamiento de datos personales, eximiendo a FIMABIS-IBIMA,, de cualquier responsabilidad en este sentido. En todo caso consiente, al facilitar dichas referencias, a que FIMABIS-IBIMA, pueda ponerse en contacto con los mismos para poder verificar y obtener mayor información.

¿Durante cuánto tiempo vamos a conservar los datos personales

En virtud de la política de conservación de FIMABIS-IBIMA,, los datos de carácter personal serán conservados durante el plazo máximo de un año desde la recepción de los Currículums Vitae, actualice sus datos o revoque su consentimiento.

¿Cuáles son sus derechos en relación con el tratamiento de datos personales?

Puede, en cualquier momento, ejercitar los derechos que la legislación dispone, dirigiéndose de forma y modo fehaciente, a la entidad o su DPD.

Si considera que sus derechos han sido vulnerados, o no atendidos adecuadamente, puede presentar una reclamación frente a la Agencia Española de Protección de Datos (www.agpd.es).

¿A qué destinatarios se comunicarán tus datos?

Solo en los casos en los que sea exigido por la Ley o FIMABIS-IBIMA, recabe su consentimiento, sus datos podrán ser comunicados a terceros. Se señala que, en base a la legislación de transparencia, los procesos de selección pueden ser publicados en los medios de comunicación de la Entidad

Puede obtener más información https://www.ibima.eu/aviso-legal/ www.fimabis.org , registro de actividades

Conteste a este correo con ACEPTO EL TRATAMIENTO DE LOS DATOS PROPORCIONADOS, de no recibir su contestación los datos proporcionados, incluida su dirección de correo electrónico, serán cancelados y destruidos

ÍNDICE

iv.2.ii.- CLAUSULA INFORMATIVA EN APLICACIÓN web para envío de CV

Le informamos que sus datos personales, serán tratados por Fundación para la Investigación de Málaga en Biomedicina y Salud -FIMABIS- **Instituto de Investigación Biomédica de Málaga y Plataforma en Nanomedicina** -IBIMA Plataforma BIONAND-, con la finalidad de gestionar los procesos de selección de los puestos vacantes que genere la entidad. Este tratamiento de datos es necesario para la aplicación de medidas precontractuales (toma de decisiones previa a la contratación laboral) y usted consiente expresamente el mismo. No se realizarán cesiones de datos de sus datos personales.
Igualmente, le informamos que, transcurrido el proceso de selección, si no ha sido seleccionado, su currículum vitae se conservará únicamente a efectos de auditorías de la Organización y, en todo caso, sus datos serán eliminados transcurrido un año desde la finalización del proceso de selección, de no desear estar en Bolsa de Trabajo. Se señala que, en base a la legislación de transparencia, los procesos de selección pueden ser publicados en los medios de comunicación de la Entidad
Ud. puede ejercer los derechos que la legislación dispone, dirigiéndose a
Fundación para la Investigación de Málaga en Biomedicina y Salud -FIMABIS-
Instituto de Investigación Biomédica de Málaga y Plataforma en Nanomedicina -IBIMA Plataforma BIONAND-
Ins. Reg. Fundaciones Consejería Justicia y Administraciones Públicas Junta de Andalucía nº MA-606
C.I.F.: G29830643
Parque Tecnológico de Andalucía (PTA)Avenida Severo Ochoa, 35, 29590, Málaga.
tlf. 951 440 260- 951 440 263; fimabis@fimabis.org / ibima@ibima.eu
Email DPD: DPD_PROTECCIONDATOS@IBIMA.EU
de forma y modo fehaciente, acreditando debidamente su identidad. En cualquier situación, Ud. tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD).

Puede obtener más información en https://www.ibima.eu/aviso-legal/ www.fimabis.org Registro de Actividades/curriculum (Enlace a la sección de RAT concerniente al tratamiento de curriculum)

(“CHECK” DE ACEPTACIÓN DE INCLUSIÓN EN BOLSA DE TRABAJO PREVIO AL ENVIO DE CV)
(“CHECK” DE ACEPTACIÓN DE CONDICIONES PREVIO AL ENVIO DE CV)

iv.2.iii.- GRABACIÓN CLAUSULA INFORMATIVA en propuesta telefónica

Para la lícita y óptima prestación de servicios le informamos que esta conversación va a ser grabada.

Los datos personales que proporcione serán tratados por la Fundación para la Investigación de Málaga en Biomedicina y Salud -FIMABIS-, Instituto de Investigación Biomédica de Málaga y Plataforma en Nanomedicina -IBIMA Plataforma BIONAND-con la finalidad de gestionar los procesos de selección de los puestos vacantes que genere la entidad. Este tratamiento de datos es necesario para la aplicación de medidas precontractuales (toma de decisiones previa a la contratación laboral) y usted consiente expresamente el mismo. No se realizarán cesiones de datos de sus datos personales.
Igualmente, le informamos que, transcurrido el proceso de selección, si no ha sido seleccionado, su currículum vitae se conservará únicamente a efectos de auditorías de la Organización y, en todo caso, sus datos serán eliminados transcurrido un año desde la finalización del proceso de selección, de no desear estar en Bolsa de Trabajo. Se señala que, en base a la legislación de transparencia, los procesos de selección pueden ser publicados en los medios de comunicación de la Entidad
Ud. puede ejercer los derechos que la legislación dispone, dirigiéndose a
Fundación para la Investigación de Málaga en Biomedicina y Salud -FIMABIS-
Instituto de Investigación Biomédica de Málaga y Plataforma en Nanomedicina -IBIMA Plataforma BIONAND-
C.I.F.: G29830643
Parque Tecnológico de Andalucía (PTA)Avenida Severo Ochoa, 35, 29590, Málaga.
tlf. 951 440 260- 951 440 263; fimabis@fimabis.org / ibima@ibima.eu
Email DPD: DPD_PROTECCIONDATOS@IBIMA.EU
de forma y modo fehaciente, acreditando debidamente su identidad. En cualquier situación, Ud. tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD).

ÍNDICE

Puede obtener más información en https://www.fiiapp.org/politica-de-privacidad/ Registro de Actividades/curriculum

iv.2.iiii.- FORMULARIO DE INFORMACIÓN Y CONSENTIMIENTO. Presentación personal

D/Dª…… con DNI…….. y dirección de contacto……, tlf…… Con interés en la presentación de mi CV, para Bolsa de trabajo/Solicitud de puesto de trabajo en Fundación para la Investigación de Málaga en Biomedicina y Salud -FIMABIS-, Instituto de Investigación Biomédica de Málaga y Plataforma en Nanomedicina -IBIMA Plataforma BIONAND-

DECLARO

Haber sido informado/a de las condiciones de tratamiento y política de privacidad de la Entidad, ACEPTANDO y CONSINTIENDO el tratamiento de los datos proporcionados, para la finalidad descrita de bolsa de trabajo/contratación

En……a……..de…….de……..

Fdo.

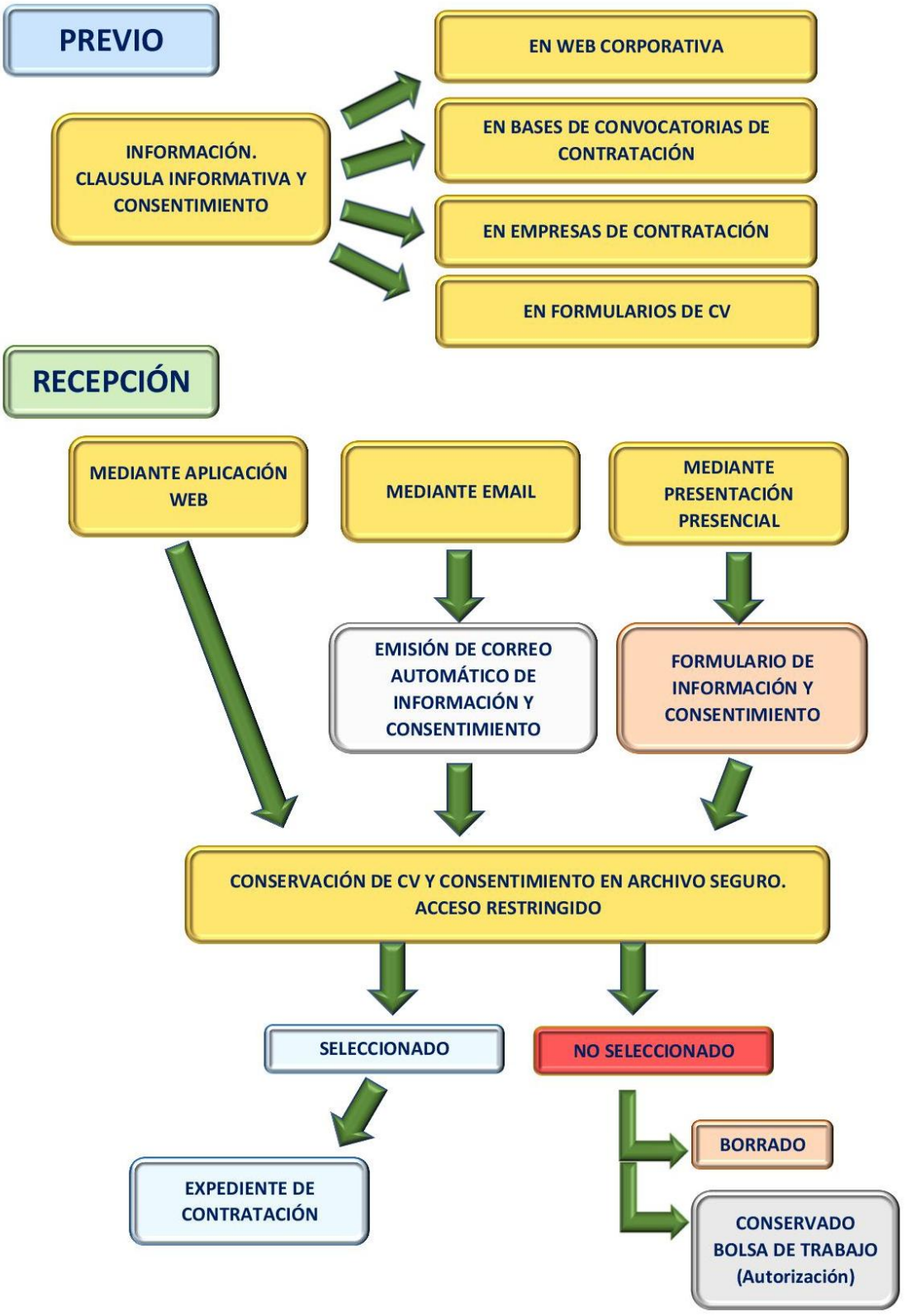
(Reverso:)

ÍNDICE (Reverso)

a) Responsable	**Fundación para la Investigación de Málaga en Biomedicina y Salud -FIMABIS-** Instituto de Investigación Biomédica de Málaga y Plataforma en Nanomedicina -IBIMA Plataforma BIONAND- Ins. Reg. Fundaciones Consejería Justicia y Administraciones Públicas Junta de Andalucía nº MA-606 C.I.F.: G29830643 Parque Tecnológico de Andalucía (PTA)Avenida Severo Ochoa, 35, 29590, Málaga. tlf. 951 440 260- 951 440 263; fimabis@fimabis.org / ibima@ibima.eu
b) Delegado de protección de datos	DPD_PROTECCIONDATOS@IBIMA.EU
c) **Base jurídica**	**RGPD: 6.1** a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. b) Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales. **Legislación vinculada:** Real Decreto Legislativo 2/2015, Ley del Estatuto de los Trabajadores. Ley 19/2013, de transparencia, acceso a la información pública y buen gobierno.
d) **Fines del tratamiento**	Gestión de solicitudes de empleo, bolsa de trabajo y curriculum personales.
e) **Colectivo**	Personal Solicitante
f) **Categorías de Datos**	Nombre y apellidos, DNI/Documento identificativo. Datos de contacto: dirección, email y teléfono. Datos de características personales: estado civil, nacionalidad, fecha y lugar de nacimiento. Datos académicos y profesionales: Titulaciones, formación y experiencia profesional.
g) **Categoría destinatarios**	Sin cesiones previstas, salvo exigencia legal Se señala que, en base a la legislación de transparencia, los procesos de selección pueden ser publicados en los medios de comunicación de la Entidad
h) **Transf. Internacional**	No están previstas transferencias internacionales de los datos. No obstante, dado el ámbito internacional de la entidad podrán comunicarse a sus sedes para la gestión de puestos de trabajo específicos.
i) **Plazo supresión**	Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. En todo caso 12 meses, de no mediar actualización o requerimiento de cancelación o supresión.
j) **Medidas de seguridad**	Las medidas de seguridad implantadas se corresponden con las previstas en el Reglamento Europeo 2016/679 de protección datos de carácter personal y L.O.P.D.G.D.D. 3/2018, y ENS Control de accesos y autorizaciones. Seguridad física infraestructuras y edificios Seguridad lógica de sistemas. Seguridad de redes Compromiso fehaciente de confidencialidad por parte del personal
k) Ejercicio de derechos	**Fundación para la Investigación de Málaga en Biomedicina y Salud -FIMABIS-** Instituto de Investigación Biomédica de Málaga y Plataforma en Nanomedicina -IBIMA Plataforma BIONAND- C.I.F.: G29830643 Parque Tecnológico de Andalucía (PTA)Avenida Severo Ochoa, 35, 29590, Málaga. tlf. 951 440 260- 951 440 263; fimabis@fimabis.org / ibima@ibima.eu Solicitud de tutela ante la Agencia Española de Protección de Datos. www.aepd.es
l) Más información	https://www.ibima.eu/aviso-legal/ www.fimabis.org

ÍNDICE

V.- ESQUEMA RESUMEN



ÍNDIC

ANEXO E .- PROTOCOLO EN EL TRATAMIENTO DE DATOS DE SALUD

I.- BREVE INTRODUCCIÓN NORMATIVA:

Junto a los principios generales de protección de datos de carácter personal ya considerados, se debe tener presente lo establecido específicamente en la normativa vinculada a la investigación y docencia biomédica, así:

Ley 41/2002, básica reguladora de la autonomía del paciente.

Artículo 7. El derecho a la intimidad.

1. Toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley.

2. Los centros sanitarios adoptarán las medidas oportunas para garantizar los derechos a que se refiere el apartado anterior, y elaborarán, cuando proceda, las normas y los procedimientos protocolizados que garanticen el acceso legal a los datos de los pacientes.

LEY 14/2007, de 3 de julio, de Investigación biomédica.

Art.5. Protección de datos personales y garantías de confidencialidad"

1.- Se garantizará la protección de la intimidad personal y el tratamiento confidencial de los datos personales que resulten de la actividad de investigación biomédica, conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (se debe referenciar a la nueva normativa).

3.- Se prohíbe la utilización de datos relativos a la salud de las personas con fines distintos a aquéllos para los que se prestó el consentimiento.

4.- Quedará sometida al deber de secreto cualquier persona que, en el ejercicio de sus funciones en relación con una actuación médico-asistencial o con una investigación biomédica, cualquiera que sea el alcance que tengan una y otra, acceda a datos de carácter personal. Este deber persistirá aún una vez haya cesado la investigación o la actuación.

Artículo 9. Límites de los análisis genéticos.

1. Se asegurará la protección de los derechos de las personas en la realización de análisis genéticos y del tratamiento de datos genéticos de carácter personal en el ámbito sanitario.

Artículo 15. Información a los sujetos participantes en la investigación.

1. Las personas a las que se solicite su participación en un proyecto de investigación recibirán previamente la necesaria información, debidamente documentada y en forma comprensible y cuando se trate de personas con discapacidad de forma adecuada a sus circunstancias.

2. La información incluirá el propósito, el plan detallado, las molestias y los posibles riesgos y beneficios de la investigación. Dicha información especificará los siguientes extremos:(…)

d) Medidas para asegurar el respeto a la vida privada y a la confidencialidad de los datos personales de acuerdo con las exigencias previstas en la legislación sobre protección de datos de carácter personal.

Artículo 50. Acceso a los datos genéticos por personal sanitario.

2. Los datos genéticos de carácter personal sólo podrán ser utilizados con fines epidemiológicos, de salud pública, de investigación o de docencia cuando el sujeto interesado haya prestado expresamente su consentimiento, o cuando dichos datos hayan sido previamente anonimizados.

Artículo 58.1 la obtención de muestras biológicas con fines de investigación biomédica podrá realizarse únicamente cuando se haya obtenido previamente el consentimiento escrito del sujeto fuente y previa información de las consecuencias y los riesgos que pueda suponer tal obtención para su salud. Dicho consentimiento será revocable

Artículo 59. Información previa a la utilización de la muestra biológica.

1. Sin perjuicio de lo previsto en la legislación sobre protección de datos de carácter personal, y en particular, en el artículo 45 de esta Ley, antes de emitir el consentimiento para la utilización de una muestra biológica con fines de investigación biomédica que no vaya a ser sometida a un proceso de anonimización, el sujeto fuente recibirá la siguiente información por escrito: (…).

c) Posibles inconvenientes vinculados con la donación y obtención de la muestra, incluida la posibilidad de ser contactado con posterioridad con el fin de recabar nuevos datos u obtener otras muestras.

e) Derecho de revocación del consentimiento y sus efectos, incluida la posibilidad de la destrucción o de la anonimización de la m uestra y de que tales efectos no se extenderán a los datos resultantes de las investigaciones ya realizadas.

f) Lugar de realización del análisis y destino de la muestra al término de la investigación: disociación, destrucción, u otras investigaciones, y que, en su caso, comportará a su vez el cumplimiento de los requerimientos previstos en esta Ley. En el caso de que estos extremos no se conozcan en el momento, se establecerá el compromiso de informar sobre ello en cuanto se conozca.

g) Derecho a conocer los datos genéticos que se obtengan a partir del análisis de las muestras donadas.

ÍNDICE

h) Garantía de confidencialidad de la información obtenida, indicando la identidad de las personas que tendrán acceso a los datos de carácter personal del sujeto fuente.

Real Decreto 1090/2015, de 4 de diciembre, por el que se regulan los ensayos clínicos con medicamentos, los Comités de Ética de la Investigación con medicamentos y el Registro Español de Estudios Clínicos

Artículo 39. Promotor.

3. Son responsabilidades del promotor:

a) Establecer y mantener un sistema de garantías y control de calidad, con procedimientos normalizados de trabajo escritos, de forma que los ensayos sean realizados y los datos generados, documentados y comunicados de acuerdo con el protocolo, las normas de buena práctica clínica y lo dispuesto en este real decreto. Deberá disponer de procedimientos normalizados de trabajo que garanticen estándares de calidad en todas las fases de la documentación de un acontecimiento adverso, recogida de datos, validación, evaluación, archivo, comunicación y seguimiento.

Artículo 41. Investigador.

3. Son responsabilidades del investigador:

c) Garantizar que el consentimiento informado se recoge de conformidad a lo establecido en este real decreto.

g) Garantizar que todas las personas implicadas respetarán la confidencialidad de cualquier información acerca de los sujetos del ensayo, así como la protección de sus datos de carácter personal.

6. El personal contratado debe ser autorizado por la dirección del centro sanitario, especificando si tiene o no acceso a la historia clínica y datos de carácter personal de los sujetos incluidos en el ensayo. Esta autorización puede materializarse de dos formas, mediante:

a) La firma de un contrato, si es personal contratado por el centro.

b) Documento independiente de acceso si es personal contratado por terceros.

Orden SSI/81/2017, de 19 de enero, pautas básicas destinadas a asegurar y proteger el derecho a la intimidad del paciente por los alumnos y residentes en Ciencias de la Salud.

7.2.1 La LBAP en su artículo 16.3 establece que el acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico asistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.

La disociación de datos obliga a separar los datos de utilidad científica (clínico-asistenciales en nuestro caso) de aquellos otros que permitan identificar a su titular (número de historia clínica, de la Seguridad Social, DNI, etc.). La disociación de datos habrá de realizarla un profesional sanitario sujeto al secreto profesional u otra persona sujeta a una obligación equivalente de secreto.

En el ámbito de la docencia los alumnos podrán acceder a la historia clínica con datos personales disociados o historias clínicas simuladas por el responsable de docencia a fin de garantizar que el aprendizaje derivado de las mismas se realiza respetando la intimidad y confidencialidad de los datos de salud.

8.2 Tanto residentes como alumnos están sometidos al deber de confidencialidad/secreto, no solo durante la estancia en el Centro sanitario en el que se esté formando sino también una vez concluida la misma, sin que dicho deber se extinga por la defunción del paciente.

El deber de confidencialidad afecta no solo a «datos íntimos» (incluidos los psicológicos relativos a ideas, valores, creencia, vivencias personales…) sino también a datos biográficos del paciente y de su entorno (sean íntimos o no) cuyo conocimiento por terceros pueda afectar a los derechos de la persona objeto de tratamiento.

El deber de confidencialidad/secreto no solo se refiere a los datos contenidos en la historia clínica del paciente sino también a los que se ha tenido acceso mediante comunicación verbal, grabaciones, videos, así como a los contenidos en cualquier tipo de archivo informático, electrónico, telemático o registro público o privado, incluidos los referidos al grado de discapacidad e información genética.

8.3 A tal fin todo el personal en formación suscribirá al inicio de su estancia en el centro sanitario, donde se esté formando, un compromiso de confidencialidad (ver modelo indicativo en los Anexos I y II) que constará en el Libro Registro para el personal investigador y en régimen de alumnado al que se refiere el apartado 9, y en el caso de los especialistas en formación en los expedientes personales de los mismos que custodia la Comisión de Docencia.

ÍNDICE

Por último, señalar que el artículo 197 apartados 1 y 2 del Código Penal castiga tanto «al que descubra secretos o vulnere la intimidad de otro sin su consentimiento» (incluyendo grabaciones, reproducciones de escucha, sonido e imágenes) como al que «sin estar autorizado se apodere de datos

reservados de carácter personal de otro que se hallen registrados en cualquier tipo de registro público o privado». Y paralelamente, el artículo 199 se refiere al deber de secreto profesional castiga «al que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales».

II.- LOS DATOS DE CARÁCTER PERSONAL EN LA INVESTIGACIÓN Y DOCENCIA BIOMÉDICA

En lo programas y proyectos de investigación y docencia, en el ámbito biomédico, se tratan datos de "salud", no obstante, esta terminología, tanto "dato personal" como "tratamiento", precisan de una clara caracterización.

Se define como "datos personales": toda información sobre una persona física identificada o identificable (el/la interesado/a); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Así, valores o parámetros analíticos, no son en sí mismos datos personales, incluso imágenes radiológicas o ecográficas, que no lleven identificación, difícilmente se pueden considerar "datos personales".

Por otro lado, y en paralelo, el tratamiento de muestras biológicas, susceptibles de discriminación genética, si entran dentro del concepto de datos personales, la normativa define "datos genéticos": como datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

Hay que valorar el riesgo que puede entrañar la identificación genética y la posible, aunque ilícita, creación de listados o ficheros en base a dicha información.

En otro ámbito, reseñar, que los datos de investigadores/as, personal laboral, o representantes de entidades, son datos vinculados a su propia actividad y en buena medida no sujetos a la normativa de protección de datos, siempre que su uso, tratamiento o finalidad sea consecuencia directa de la actividad para la cual fueron proporcionados. En este sentido:

RGPD. Considerando (14) …. El presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto.

RESOLUCIÓN Nº.: R/01690/2018 (AEPD): (…) En definitiva, pues, tanto las personas jurídicas como los profesionales que presten sus servicios en aquéllas quedan fuera del ámbito competencia del RGPD.

Es de destacar el tratamiento de **DATOS DE MENORES** de 14 años, la LOPDGDD 3/2018, señala:

Artículo 7. Consentimiento de los menores de edad.

1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

Todo ello, siempre teniendo en consideración el principio del "interés superior del/de la menor" reconocido expresamente en la Ley Orgánica 1/1996 de 15 de enero, de protección jurídica del/de la menor, de darse tal interés (lo cual es ponderable en el caso de que nos atañe de investigación biomédica).

Pero hay que tener en consideración, que el consentimiento puede no ser unívoco por parte de los progenitores/tutores, si bien el Código Civil en su art. 156, reseña: *La patria potestad se ejercerá conjuntamente por ambos progenitores o por uno solo con el consentimiento expreso o tácito del otro. Serán válidos los actos que realice uno de ellos conforme al uso social y a las circunstancias o en situaciones de urgente necesidad*.

El consentimiento, en este ámbito, exige según lo establecido por el RGPD en su art. 8.2. que *el responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento*

ÍNDICE

fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.
De lo anterior cabe deducir que se deberá contar con el consentimiento de toda aquella persona que ostente la patria potestad y/o representación fehaciente del7de la menor, comprobándose tales extremos de forma adecuada.

III.- ACTUACIONES

Partiendo de lo señalado, a la hora de tratar datos para una investigación, se debe tener claro, qué datos se necesitan y cuál es su finalidad, en este sentido cabe recordar los principios que deben regir el tratamiento de datos de carácter personal, así:
Los datos personales serán:

- ✓ *tratados de manera lícita, leal y transparente en relación con el interesado **(«licitud, lealtad y transparencia»**);*
- ✓ *recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales **(«limitación de la finalidad»);***
- ✓ *adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados **(«minimización de datos»);***
- ✓ *exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan **(«exactitud»);***
- ✓ *mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado **(«limitación del plazo de conservación»);***
- ✓ *tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas **(«integridad y confidencialidad»).***

Se tiene pues que discriminar el tratamiento de datos de salud, atendiendo a cuestiones fundamentales como:

- ✓ ¿Se puede singularizar(identificar) a una persona?
- ✓ ¿Se pueden vincular registros relativos a una persona?
- ✓ ¿Se puede inferir información relativa a una persona?

Y tener clara la **tipología de datos necesarios**:

- ➢ Datos identificativos directos: nombre y apellidos, dirección, número de teléfono, email, DNI, Nº tarjeta sanitaria, imagen reconocible (incluso por particularidades como tatuajes)
- ➢ Datos identificativos indirectos: Número de expediente, edad, lugar de nacimiento, sexo, localización de tratamiento/investigación...

ÍNDICE

Es importante señalar que muchos datos no directamente identificadores, pueden ser usados en conjunción con otros datos, incluso datos hechos públicos en redes sociales, para identificar a una persona.
Es por ello que el principio de minimización de la información debe ser central en cualquier tratamiento de datos.
Es obligado determinar qué datos son necesarios, y eliminar toda aquella información que no sea imprescindible para la investigación o la docencia.

Por otro lado, una vez determinados los datos objeto de tratamiento, se debe particularizar su acceso, quien debe tratar, por su asistencia y función clínica, los datos de carácter personal de los/las sujetos/pacientes, y quien no precisa de tal acceso.

El acceso, tal y como determina el art. 41.6 del Real Decreto 1090/2015, debe estar controlado por un documento de confidencialidad y responsabilidad, aun cuando esté definido el deber de secreto, así:

a) La firma de un contrato, si es personal contratado por el centro.
b) Documento independiente de acceso si es personal contratado por terceros.

Y de ser posible, la información será anonimizada o seudonimizada.

III.1.- ANONIMIZACIÓN O SEUDONIMIZACIÓN

Como señala la AEPD (https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-procedimientos-anonimizacion.pdf), la finalidad del proceso de **anonimización** es eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados manteniendo la veracidad de los resultados del tratamiento de los mismos, es decir, además de evitar la identificación de las personas, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización no conlleva una distorsión de los datos reales.

En el proceso de anonimización se deberá producir la ruptura de la cadena de identificación de las personas. Esta cadena se compone de microdatos o datos de identificación directa y de datos de identificación indirecta. Los microdatos permiten la identificación directa de las personas y los datos de identificación indirecta (Identificación indirecta: la que puede tener lugar como consecuencia de información de una o varias fuentes que por sí misma o en combinación de otros factores puede permitir la reidentificación de las personas cuando sus datos hubieran sido anonimizados. Por ejemplo, la combinación de sexo, edad, lugar de nacimiento y padecimiento de una determinada enfermedad pueden permitir la identificación indirecta de una persona concreta) son datos cruzados de la misma o de diferentes fuentes que pueden permitir la reidentificación de las personas, como la información de otras bases de datos del mismo u otro responsable, de las redes sociales, buscadores, blogs, etc.

Por su parte, **seudonimización,** es el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un/a interesado/a sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

La seudonimización consiste en la sustitución de un atributo (normalmente un atributo único) por otro en un registro. Por consiguiente, sigue existiendo una alta probabilidad de identificar a la persona física de manera indirecta; en otras palabras, el uso exclusivo de la seudonimización no garantiza un conjunto de datos anónimo.

La seudonimización reduce la posibilidad de vinculación de un conjunto de datos con la identidad del/de la interesado/a; se trata, por tanto, de una medida de seguridad útil, pero no es un método de anonimización. No obstante, es necesario en caso de que se requiera o exija la trazabilidad y restaurar la disponibilidad y el acceso a los datos personales.

ÍNDICE

III.2.- MEDIDAS BÁSICAS DE CONTROL EN EL TRATAMIENTO DE DATOS PERSONALES QUE INCLUYAN DATOS DE SALUD.

Junto a las diversas medidas recogidas en este Protocolo, se debe especialmente vigilar y cumplir:

- **Recoger el consentimiento previo** al tratamiento de datos personales. Hay que señalar, que, si bien los formatos al uso recogen en su mayor parte las exigencias tanto de la normativa de protección de datos como de las referentes a investigación y ensayos clínicos, se debe prestar especial atención:
  - información sobre las responsabilidades del personal, (recuérdense las obligaciones de Promotor e Investigador Principal),
  - riesgos en la perspectiva del tratamiento de datos personales, de la investigación genética,
  - consentimiento de los/las menores de 14 años

- **Determinar la necesidad del tratamiento de datos identificativos**. Se debe tener en cuenta, que la fecha de nacimiento, sexo, peso, patología, lugar de tratamiento/investigación, pueden en su conjunto ser datos identificativos.

- **Discriminar el personal con necesidad de acceso**. Se recogerá documento de confidencialidad/responsabilidad, o en su caso se comprobará su firma previa en documentos de contratación o proyectos de investigación.
  Todo el personal con acceso a datos de salud identificadores, está sometido al deber de secreto. Señalar que el incumplimiento de dicho deber constituye un ilícito penal (al igual que compartir conversaciones de terceros por redes sociales o whatsapp).

- No se deben enviar datos de carácter personal por correo electrónico, si no están encriptados, o mediante clave de acceso segura. Se deben emplear los correos corporativos para comunicaciones derivadas de la actividad profesional.
  Si es imprescindible el envío de datos personales, se recomienda un mínimo de **doble factor de autenticación**. Se trata de una medida de seguridad que requiere de un código obtenido a partir de una aplicación, o un mensaje “SMS” por ejemplo, además de una contraseña para acceder al fichero.
  Como ejemplo práctico y de fácil implementación, en caso necesario, se puede comprimir un archivo con herramientas como WinRAR e insertarle una contraseña, incluso encriptando el nombre del archivo, enviar dicho archivo por email, y la contraseña por teléfono.

ANEXO F.- NORMATIVA DE USO DE MEDIOS ELECTRÓNICOS

1.- OBJETIVO

1. La presente normativa ha sido aprobada por el Comité de Seguridad y entrará en vigor al día siguiente de su aprobación, hasta que sea reemplazada por una modificación o una nueva Normativa.

2.- REVISIÓN Y/O ACTUALIZACIÓN

2. Con periodicidad anual se revisará su contenido y en caso de ser necesario se procederá a su modificación, que deberán ser aprobadas por los órganos anteriormente indicados, debiendo ser difundidas entre las personas afectadas por las mismas.

3.- OBJETO

3. El objeto del presente documento es establecer la normativa de uso seguro de los medios electrónicos en la **Fundación para la Investigación de Málaga en Biomedicina y Salud (FIMABIS)**, organización dedicada a integrar armónicamente la investigación básica, clínica y de salud pública promoviendo, desarrollando y divulgando la investigación científica en el área biomédica, biosanitaria y biotecnológica, dando soporte efectivo a la innovación en ciencias de la vida y sirviendo de enlace entre centros sanitarios y de investigación y su entorno social y geográfico. FIMABIS es la actual entidad gestora del Instituto de Investigación Biomédica de Málaga y Plataforma en Nanomedicina (IBIMA Plataforma BIONAND), y que ostenta su representación; **en adelante, la Organización**, dentro del alcance señalado en el Esquema Nacional de Seguridad.

4. Los sistemas de información son elementos básicos para el desarrollo de la actividad de la Organización. Estos medios se ponen a disposición de las personas usuarias como instrumentos de trabajo para el desempeño de su actividad profesional. Motivo por el cual se deben utilizar estos recursos de manera responsable, mediante el seguimiento de normas, y buenas prácticas que salvaguarden la seguridad de la información, los sistemas de información y los recursos tecnológicos proporcionados por la entidad.

4.- ALCANCE

5. Mediante la presente normativa, la Organización establece la regulación del Uso de los Medios Electrónicos de su sistema de información (incluido el acceso remoto a los mismos), a través del establecimiento de medidas de cumplimiento obligatorio para todo el personal, quedando sujetos a la misma, así como a los principios morales y éticos en la utilización de los recursos puestos a disposición.

6. El personal de terceros (empresas proveedoras, convenios, etc.) con acceso al sistema quedan también sujetos a la misma, en la medida que le sean de aplicación, así como a los principios morales y éticos en la utilización de los recursos puestos a disposición de estas personas usuarias para el desempeño de sus actividades en la Organización.

7. En adelante, se utilizará “el Usuario” para referirse al personal propio o de terceros.

5.- CANAL DE SOLICITUDES Y/O NOTIFICACIONES

8. Las solicitudes de autorización y las notificaciones reflejadas en esta normativa se dirigirán mediante correo electrónico al Responsable de Sistemas de la Fundación.

6.- INCIDENTES DE SEGURIDAD

9. Cuando un Usuario detecte cualquier anomalía (mal funcionamiento, aplicaciones que no arrancan o que se cierran de manera inesperada, pérdida de documentos, de memorias USB, etc.) o incidente de seguridad (virus, suplantación de identidad, pérdidas de clave, etc.) que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información de la Organización o pueda dañar a su imagen, deberá informar inmediatamente.

7.- NORMATIVA DE USO DE MEDIOS ELECTRÓNICOS

7.1.- NORMAS DE UTILIZACIÓN DEL EQUIPAMIENTO INFORMÁTICO Y DE COMUNICACIONES

10. Estas normas conciernen específicamente a todos los dispositivos facilitados y configurados por la Organización, incluyendo equipos de sobremesa, portátiles y dispositivos móviles con capacidades de acceso a los Sistemas de Información.

11. La Organización proporcionará al personal, el equipamiento debidamente configurado con acceso a los servicios y aplicaciones que sean necesarios para el desempeño de sus funciones.

12. Respecto a los cuales aplicará las normas generales y para los equipos portátiles y dispositivos móviles aplicará las normas específicas para este tipo de equipamiento.

7.1.1.- 8.1.1 Normas Generales

13. Los equipos deberán de utilizarse únicamente para fines institucionales profesionales y como herramienta para el desempeño de las tareas encomendadas. Cada equipo estará asignado a una única persona. Esta persona es responsable de su correcto uso.

• Salvo autorización expresa, no se dispondrán de privilegios de administrador sobre los equipos.

• Únicamente el personal autorizado podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos.

• Cuando sea necesario instalar equipos que no hayan sido provistos por la Organización deberá de solicitarse autorización previa.

14. Las personas usuarias deberán notificar, a la mayor brevedad posible, cualquier comportamiento anómalo de sus equipos (va lento, no arranca, no funciona correctamente, etc.), especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo. Del mismo modo deberá de comunicar la ausencia de cables y/o accesorios o cualquier otra evidencia de deterioro del mismo.

15. Con carácter general, no está permitido el uso de dispositivos propios, "BYOD (Bring Your Own Device)", para el acceso o almacenamiento de información salvo autorización expresa.

7.1.2.- 8.1.2 Normas específicas para equipos portátiles y dispositivos móviles

16. Para los portátiles y móviles además de las normas generales, serán de aplicación la siguientes:

17. Estos dispositivos estarán, en todo momento bajo la custodia de la persona usuaria que los utilice, que será la responsable de adoptar las medidas necesarias para evitar daños o sustracción, así como del acceso a ellos por parte de personas no autorizadas.

• La sustracción de estos equipos se ha de notificar inmediatamente para la adopción de las medidas que correspondan.

• Se debe solicitar autorización cuando se usen para conectarse remotamente a través de redes que no estén bajo el control de la organización o que no hayan sido autorizadas, autorización que se hará extensible también a los servicios a los que se accede.

18. Cuando se modifiquen las circunstancias profesionales (término de una tarea, cese en el cargo, etc.) que originaron la entrega de un recurso informático móvil, la persona usuaria lo devolverá, al objeto de proceder al borrado seguro de la información almacenada y restaurar el equipo a su estado original para que pueda ser asignado a una nueva persona.

7.2.- NORMAS PARA EL ALMACENAMIENTO DE INFORMACIÓN Y COPIAS DE SEGURIDAD

19. Para garantizar la disponibilidad de la información frente a un incidente de seguridad, de forma periódica se realizan copias de seguridad de las bases de datos y fuentes de los programas que se utilicen dentro de la organización.

20. Por este motivo, los Usuarios deberán almacenar en estas los datos generados en el desempeño de sus competencias profesionales. A este respecto, se informa que no se realizan copias de seguridad de la información que no se encuentren en las unidades indicadas.

21. No está permitido el almacenamiento de información privada ni de terceros ajenos en los recursos indicados.

22. La información almacenada en las copias de seguridad podrá ser recuperada en caso de que se produzca algún incidente de seguridad. Para recuperar esta información se habrá de dirigir una solicitud de restauración.

7.3.- NORMAS DE USO PARA SOPORTES DE ALMACENAMIENTO EXTRAÍBLES

23. Como norma general, en la Organización el uso de soportes o medios de almacenamiento extraíbles (memorias USB, discos duros, etc.) no está autorizado. Para su utilización se deberá de contar con la debida autorización.

24. En el caso de que a la persona usuaria se le autorice el uso de este tipo de soportes trabajo, las normas a observar las siguientes:

• Como norma general, se utilizarán los soportes extraíbles proporcionados por la Organización. Estando destinados a un uso exclusivamente profesional, como herramienta de transporte puntual de ficheros, no como herramienta de almacenamiento.

• El uso de medios de almacenamiento extraíbles particulares, no está autorizado, salvo que se disponga de la debida autorización.

• Su uso no está autorizado para el almacenamiento de datos personales, salvo que se disponga de la debida autorización.

25. Este tipo de dispositivos deberá de almacenarse en lugares seguros, al objeto de prevenir robos o el acceso de terceros no autorizados. La pérdida o sustracción de estos dispositivos, con indicación de su contenido, deberá ponerse en conocimiento, de forma inmediata.

26. El transporte de estos soportes fuera de las instalaciones de la Organización deberá ser realizado exclusivamente por personal autorizado, autorización que contemplará igualmente a la propia información que sale. En cuyo caso se deberá de enviar una solicitud para que se le asesore sobre las medidas de seguridad que será necesario implementar.

7.3.1.- Normas para el borrado y eliminación de soportes informáticos

27. Los medios de almacenamiento que, por obsolescencia o degradación, pierdan su utilidad, y especialmente aquellos que contengan datos de carácter personal, deberán ser eliminados de forma segura para evitar accesos a dicha información. En este sentido, la persona usuaria deberá tener en cuenta las siguientes indicaciones:

• Asegurarse que el contenido del soporte puede ser eliminado.

• Cualquier petición de eliminación de soporte informático deberá ser solicitada.

28. Para la reutilización de medios de almacenamiento, para otros fines diferentes de los que originaron su uso deberá solicitarse un borrado seguro de mismo.

8. NORMAS RESPECTO A LA GESTIÓN DE DOCUMENTOS

8.1 Impresoras en red, fotocopiadoras/escáneres

29. Con carácter general, deberán utilizarse las impresoras en red y las fotocopiadoras corporativas. Excepcionalmente, podrán instalarse impresoras locales, gestionadas por un puesto de trabajo de usuario. En este caso, la instalación irá precedida de la autorización pertinente.

30. En ningún caso se podrá hacer uso de impresoras, fotocopiadoras que no hayan sido proporcionados por la Organización. Con relación a los sistemas de copia e impresión y documentación impresa, los Usuarios debe seguir las siguientes directrices:

31. Los documentos, con carácter general, se generarán en formato electrónico, pudiendo digitalizar aquellos que no sean susceptibles de ser generados en el citado formato.

• Cuando se impriman documentos, en sistemas de impresión o copia comunes, éstos deberán permanecer el menor tiempo posible en las bandejas de salida de las impresoras, para evitar que terceras personas puedan acceder a la misma.

• En la realización de copias de documentos y/o escaneo, no debe olvidarse retirar los originales.

• En caso de encontrase documentación en un sistema de copia o impresión, el Usuario intentará localizar a la persona propietaria para que proceda a su recogida inmediata. En caso de desconocer a la persona propietaria o no estar localizable, lo pondrá inmediatamente en conocimiento.

• Para evitar un uso excesivo de los recursos, mejorando el impacto medioambiental en la generación de documentos en papel, y por motivos de seguridad, antes de imprimir documentos, el Usuario debe asegurarse de que es absolutamente necesario hacerlo.

8.2 Cuidado y protección de la documentación impresa

32. La documentación debe ser protegida, de forma que sólo tenga acceso a ella el personal autorizado, a tal efecto la persona usuaria tendrá en cuenta las siguientes medidas:

• Los puestos de trabajo permanecerán despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.

33. Cuando no vaya a ser utilizada se deberá guardar en sistemas de almacenamiento (armarios o archivadores) preferentemente bajo llave. No podrán ser publicados en tablones o similares.

• Cuando los documentos no sean necesarios, deberán ser eliminados utilizando para ello los medios puestos a disposición por parte de la entidad (destructora de documentos) de forma que no sea recuperable la información que pudieran contener.

• Antes de abandonar las salas de reuniones o permitir que alguien ajeno acceda a las mismas, se limpiarán adecuadamente las pizarras y se recogerán todos los documentos, cuidando de que no quede ningún tipo de información “sensible” o “interna” accesible a personas no autorizadas.

8.3 Puesto de trabajo despejado

34. Los puestos de trabajo deben permanecer despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.

9.- ACCESO A LOS SISTEMAS DE INFORMACIÓN Y A LOS DATOS TRATADOS

35. Para acceder a los sistemas y recursos informáticos es necesario tener asignada previamente una cuenta de usuario. El alta de los usuarios será solicitada y autorizada de acuerdo con las políticas de la organización. La autorización del acceso establecerá el perfil necesario con el que se configuren las funcionalidades y privilegios disponibles en las aplicaciones según las competencias de cada persona, adoptando una política de asignación de privilegios mínimos necesarios para la realización de las funciones encomendadas.

36. Los Usuarios dispondrán de credenciales personales de acceso (código de usuario y una contraseña, certificado electrónico, etc.) para el acceso a los sistemas de información de la Organización **empleando la red segura, protegida con los servicios de seguridad destinados a tal efecto**, siendo responsables de su custodia y de toda actividad relacionada con el uso de su acceso autorizado, respecto de los que deberá de observar las siguientes medidas:

• El código de usuario es único para cada persona, intransferible e independiente del PC o terminal desde el que se realiza el acceso.

• Los usuarios no deben revelar o entregar, bajo ningún concepto, sus credenciales de acceso a otra persona, ni mantenerlas por escrito a la vista o al alcance de terceros. De igual modo, no deben utilizar ningún acceso autorizado de otra persona, aunque dispongan de la autorización de su titular.

• Si una persona tiene sospechas de que sus credenciales están siendo utilizadas por otra persona, debe comunicarlo inmediatamente.

• Las personas usuarias deben utilizar contraseñas seguras, de acuerdo con la política establecida en la Organización, no deben estar compuestas únicamente por palabras del diccionario u otras fácilmente predecibles o asociables a la persona usuaria (nombres de su familia, direcciones, matrículas de coche, teléfonos, nombres de productos comerciales u organizaciones, identificadores de usuario, de grupo o del sistema, DNI, etc.).

• Los sistemas que así lo permitan, forzarán el cambio de la contraseña al menos una vez al año, previo aviso con los suficientes días de antelación. En los que no sea posible será responsabilidad de los Usuarios proceder a su cambio en dicha periodicidad.

9.1.- Acceso a una cuenta de un usuario en su ausencia o baja

37. Cuando sea necesario acceder a la carpeta personal o cuenta de correo corporativa de un Usuario, este acceso se deberá realizar contando con la autorización expresa de la persona titular de las misma (la Organización) y solo podrá ser realizado por el Responsable de la misma, o por la persona en que esta delegue.

38. En caso de que no resulte posible recabar esta autorización (fallecimiento, enfermedad, imposibilidad de localización, etc.), el acceso podrá ser realizado siempre y cuando esté autorizado de forma expresa por el por el Responsable del mismo o por la persona en que esta delegue.

39. En ambos casos, se deberá motivar la necesidad de acceso y ser comunicada al Responsable del Usuario, que procederá a la elaborando un acta en el que se recojan todas las acciones llevadas a cabo.

10. CONFIDENCIALIDAD, PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y DEBER DE SECRETO

40. La información contenida en el Sistema de Información de la Organización es responsabilidad de dicha entidad, por lo que las personas usuarias deben abstenerse de comunicar, divulgar, distribuir o poner en conocimiento o al alcance de terceros (externos o internos no autorizados) dicha información, salvo autorización expresa de la propia Institución. Además, deberá de tener en cuenta las siguientes premisas:

• Todas los Usuarios, que por razón de su actividad profesional hubiera tenido acceso a información gestionada por la Organización (documentos, metodologías, claves, análisis, programas, etc.) deberán mantener sobre ella, por tiempo indefinido, una absoluta reserva.

• Los Usuarios solo podrán acceder con las debidas autorizaciones a aquella información necesaria para el desempeño de sus labores. En todo caso, no deberá acceder a información sin las debidas autorizaciones.

41. Toda información contenida en los sistemas de información de la Organización o que circule por sus redes de comunicaciones debe ser utilizada únicamente para el cumplimiento de las funciones que tiene encomendadas el Usuario.

• Los derechos de acceso de los Usuarios a la información y a los sistemas de información que la tratan deberán siempre otorgarse en base a los principios de "mínimo privilegio", "necesidad de conocer y responsabilidad de compartir" y "capacidad de autorizar".

42. La información que comprenda datos de carácter personal quedará afectada también por la normativa vigente en materia de Protección de Datos personales, estando obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con la Organización.

11. LIMPIEZA DE METADATOS Y DATOS OCULTOS DE LOS DOCUMENTOS ELECTRÓNICOS

43. Se define **metadato** como información estructurada que describe, explica, localiza y además hace más fácil recuperar, utilizar o gestionar un recurso de información. Los metadatos son comúnmente llamados "datos sobre los datos" o "información sobre la información".

44. Se define información o **datos ocultos** como aquellos datos existentes en el contenido de los documentos electrónicos, que no son visibles con la configuración estándar o configuración por defecto de los programas utilizados para su creación y tratamiento, siendo necesario aplicar alguna opción específica dentro de la configuración de estos programas, para su visualización. Un ejemplo de datos ocultos es el texto oculto, filas o columnas ocultas, comentarios o información del documento, etc.

45. Cuando hacemos una fotografía o creamos documentos con aplicaciones de Microsoft Office (Word, Excel, PowerPoint, etc.), estos archivos llevan integrados en sus propiedades una serie de datos ocultos y/o metadatos, como pueden ser el nombre de la persona que ha creado el documento, el programa con el que se ha generado, la fecha de creación, la de modificación, etc. Esto puede perjudicar a la confidencialidad de la información y a la buena imagen de la Organización.

46. Todos los archivos electrónicos (documentos ofimáticos, hojas de cálculo, imágenes, etc.) pueden tener integrados en sus propiedades una serie de datos ocultos y/o metadatos, como pueden ser el nombre de la persona que ha creado el documento, el programa con el que se ha generado, la fecha de creación, la de modificación, etc.

47. Los metadatos contenidos en los archivos pueden llegar a afectar tanto a la seguridad de la información como a la imagen de la Organización. Por ello, todo archivo que vaya a ser difundido internamente, remitido electrónicamente a un tercero o publicado en Internet (página web, sede electrónica, etc.), deberá ser revisado para determinar los metadatos asociados al mismo, procediendo a su modificación o supresión, si procede, siguiendo el procedimiento establecido en el anexo "Procedimiento de Limpieza de Metadatos".

12. USO DEL CORREO ELECTRÓNICO CORPORATIVO

48. El correo electrónico corporativo es una herramienta de mensajería electrónica centralizada, puesta a disposición de los Usuarios del sistema de información de la Organización para el envío y recepción de correos electrónicos mediante el uso de cuentas de correo corporativas. Al tratarse de un recurso compartido, un uso indebido del mismo repercute de manera directa en el servicio ofrecido a todas las personas.

49. El correo electrónico se deberá emplear en base al "sentido común" y teniendo en cuenta la responsabilidad y funciones desempeñadas, tratando en cualquier caso de no poner en compromiso ni los sistemas ni la imagen de la Organización.

50. La Organización queda facultada para filtrar el contenido del correo electrónico de la cuenta de correo proporcionada para el desarrollo de sus funciones laborales, al objeto de prevenir virus o en el supuesto de que existan razones fundamentadas en una firme sospecha por del a Organización sobre la existencia de actividades delictivas o dolosas del personal.

51. El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de la presente Normativa.

52. Se podrá insertar contenido adicional en los mensajes enviados con objeto de advertir a los receptores de los requisitos legales y de seguridad que deberán cumplir en relación con dichos correos.

53. Las características peculiares de este medio de comunicación (universalidad, bajo coste, anonimato, etc.) han propiciado la aparición de amenazas que utilizan el correo electrónico para propagarse o que aprovechan sus vulnerabilidades. Por este motivo se establecen las siguientes directrices con el objetivo de reducir el riesgo en el uso del correo electrónico:

• Utilizar el correo electrónico exclusivamente para propósitos profesionales[1].

• No se debe ceder el uso de la cuenta de correo a terceras personas[2].

54. Informar de correos con virus, phishing, malware (programa maligno), etc. Sin reenviarlos, para evitar su posible propagación.

55. No responder a mensajes de Spam[3].

• Asegurar la identidad del remitente antes de abrir un mensaje[4].

56. No ejecutar archivos adjuntos sospechosos. No deben ejecutarse los archivos adjuntos recibidos sin analizarlos previamente con la herramienta corporativa contra código malicioso[5].

57. Respecto al uso del correo electrónico, **queda terminantemente prohibido**:

• Falsificar, ocultar, suprimir o sustituir la identidad del emisor en cualquier correo electrónico.

• Leer o acceder a correos electrónicos ajenos, sin autorización previa.

• Enviar correos electrónicos que contengan en el cuerpo o en los adjuntos información con datos de categorías especiales de datos o datos especialmente sensibles (esto es, salud, ideología, religión, creencias, origen racial, étnico, etc. o aquellos considerados como de especial protección por la organización, salvo que se cuente con la autorización pertinente y se hayan aplicado las medidas de seguridad oportunas (cifrado o similares).

Así mismo, el **Anexo C "Protocolo de Gestión de Correo"** incluido en este documento recoge las directrices completas de la fundación relativas al uso del correo electrónico corporativo, estableciendo las normas de uso adecuado, las medidas de seguridad aplicables y las responsabilidades de los usuarios en la gestión de la información transmitida a través de este medio.

[1] Gran parte de los mensajes de correo electrónico no deseados, que llegan a las organizaciones tienen su origen en un uso no profesional de las cuentas de correo

[2] Esto provocaría una suplantación de identidad y el acceso a información. Es conveniente controlar la difusión de las cuentas de correo, facilitando la dirección profesional sólo en los casos necesarios y siempre y cuando el fin último sea el cumplimiento de las funciones municipales (p.e., cuando nos subscribimos a un foro).

[3] La mayor parte de los generadores de mensajes de spam (correo electrónico masivo no solicitado) se envía a direcciones de correo electrónico aleatoriamente generadas, esperando que las respuestas obtenidas confirmen la existencia de direcciones de cuentas reales. Además de ello, en ocasiones tienen el aspecto de mensajes legítimos e, incluso, pueden contener información relativa a la Corporación. En cualquier caso, nunca deben de responderse.

[4] Muchos ciberataques se originan cuando el atacante se hace pasar por una persona o entidad conocida (amigo, compañero, etc.) de la persona atacada. El origen de estas acciones es diverso: acceso no autorizado a la cuenta, suplantación visual de la identidad, introducción de código malicioso que utiliza la cuenta remitente para propagarse, etc. En caso de recibir un correo sospechoso, y dependiendo de su verosimilitud, cabe: ignorarlo, no abrirlo y poner el hecho en conocimiento del remitente, independientemente de comunicar la incidencia de seguridad correspondiente. Igualmente, el envío de información, "confidencial" a petición de un correo del que no se puede asegurar la identidad del remitente, debe rechazarse. Es importante tener en cuenta que resulta muy sencillo enviar un correo con un remitente falso. Nunca se debe confiar en que la persona con la que nos comunicamos vía email sea quien dice ser, salvo en aquellos casos que se utilicen mecanismos de firma electrónica de los correos (no sólo de los ficheros adjuntos).

[5] Esto es especialmente importante cuando se reciben adjuntos no solicitados o el correo es sospechoso. Gran parte del código malicioso suele insertarse en ficheros adjuntos, ya sea en forma de ejecutables (.exe, por ejemplo) o en forma de macros de aplicaciones (Word, Excel, etc.).

13. ACCESO A INTERNET Y OTRAS HERRAMIENTAS DE COLABORACIÓN

58. El acceso corporativo a Internet es un recurso centralizado que la Organización pone a disposición de los Usuarios, como herramienta necesaria para el acceso a contenidos y recursos de Internet y como apoyo al desempeño de su actividad profesional. La Organización velará por el buen uso del acceso a Internet, tanto desde el punto de vista de la eficiencia y productividad del personal, como desde los riesgos de seguridad asociados a su uso. Las normas de uso son las siguientes:

• Como norma general, las conexiones que se realicen a Internet deben obedecer a fines profesionales.

• Sólo se podrá acceder a Internet mediante los navegadores suministrados y configurados en los puestos de usuario. No podrá alterarse su configuración, ni utilizar un navegador alternativo, sin contar con la debida autorización.

• El sistema que proporciona el servicio de navegación podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan virus o código dañino.

59. Deberá notificarse cualquier anomalía (redirección a páginas solicitadas, aviso de sitio no seguro, en páginas habitualmente utilizadas, etc.) detectada en el uso del acceso a Internet, así como la sospecha de posibles problemas o incidentes de seguridad relacionados con dicho acceso.

60. Se consideran **usos prohibidos,** que implican un riesgo de seguridad**,** las siguientes actuaciones:

• La descarga de programas informáticos sin la autorización previa o ficheros con contenido dañino que supongan una fuente de riesgos para la organización. En todo caso debe asegurarse que el sitio Web visitado es confiable.

• El acceso, la descarga y/o el almacenamiento en cualquier soporte, de páginas con contenidos ilegales, dañinos, inadecuados o que atenten contra la moral y las buenas costumbres y, en general, de todo tipo de contenidos que incumplan las normas éticas y de cortesía de la Organización.

• El acceso a recursos y páginas web, o la descarga de programas o contenidos que vulneren la legislación en materia de Propiedad Intelectual.

• La utilización de aplicaciones o herramientas (especialmente, el uso de programas de intercambio de información, P2P) para la descarga masiva de archivos, programas u otro tipo de contenido (música, películas, etc.) que no esté expresamente autorizados.

14. MONITORIZACIÓN Y APLICACIÓN DE ESTA NORMATIVA

61. La Organización por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente:

• Revisará periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.

• Monitorizará los accesos a la información contenida en sus sistemas.

• Auditará la seguridad de las credenciales y aplicaciones.

• Monitorizará los servicios de internet, correo electrónico y otras herramientas de colaboración.

62. Esta supervisión se realizará en todo caso con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los Usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

63. Los sistemas en los que se detecte un uso inadecuado o en los que no se cumplan los requisitos mínimos de seguridad, podrán ser bloqueados o suspendidos temporalmente. El servicio se restablecerá cuando la causa de su inseguridad o degradación desaparezca.

64. El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de la presente Normativa. Se podrá insertar contenido adicional en los mensajes enviados con objeto de advertir a los receptores de los requisitos legales y de seguridad que deberán cumplir en relación con dichos correos.

65. El sistema que proporciona el servicio de navegación podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos dañino. Igualmente, el sistema podrá registrar y dejar traza de las páginas a las que se ha accedido, así como del tiempo de acceso, volumen y tamaño de los archivos descargados. El sistema permitirá el establecimiento de controles que posibiliten detectar y notificar sobre usos prolongados e indebidos del servicio.

15. INCUMPLIMIENTO DE LA NORMATIVA

66. Los Usuarios del sistema de información de la Organización están obligadas a cumplir lo prescrito en la presente Normativa de Uso de Medios Electrónicos.

67. En el supuesto de que una persona usuaria no observe alguna de los preceptos señalados en la presente Normativa, sin perjuicio de las acciones disciplinarias y administrativas que procedan y, en su caso, las responsabilidades legales correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos que tenga asignados, previa instrucción del procedimiento legal que corresponda.

68. En el caso de personal de terceros, el incumplimiento de esta normativa podría derivar en la imposición de penalidades pudiendo llegar incluso a la resolución del contrato, siguiendo el procedimiento establecido al efecto en la normativa sobre contratación administrativa.

ANEXO - PROCEDIMIENTO DE LIMPIEZA DE METADATOS

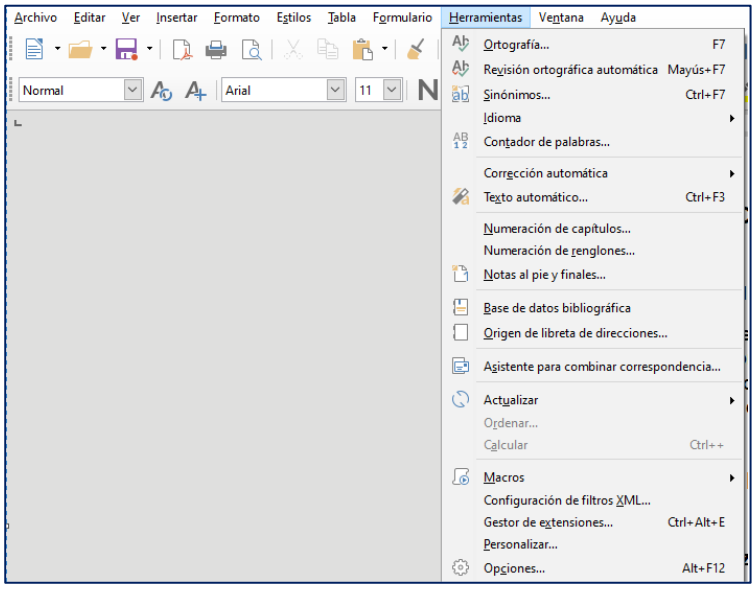
El objetivo de este anexo es describir el proceso a seguir para realizar la limpieza de los metadatos no deseados de los documentos, a realizar antes de proceder al intercambio de documento con terceros, o al subir contenidos a los entornos web.

72. METADATOS EN DOCUMENTOS DE LIBREOFFICE

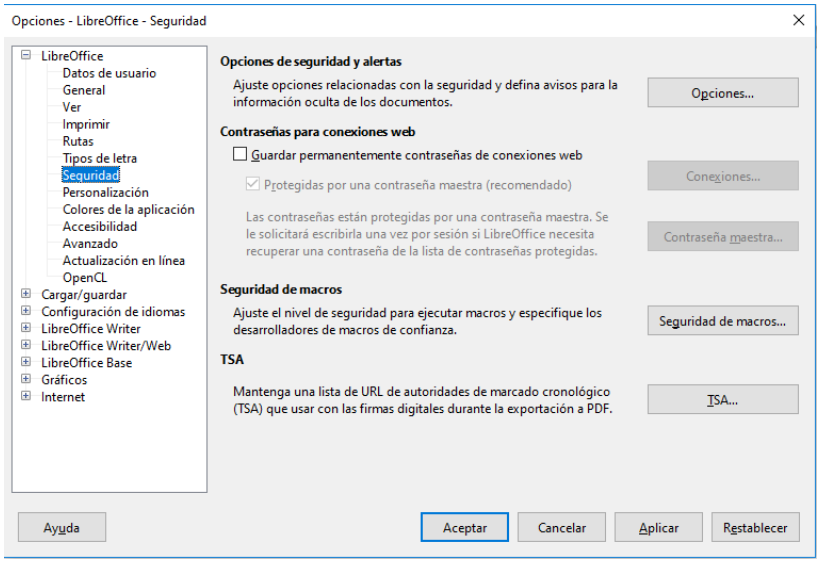
– Evitar que se guarden los metadatos en el documento

73. A continuación, se establecen las instrucciones a llevar a cabo para evitar que se guarden los metadatos en LibreOffice Versión: 6.2.5.2.

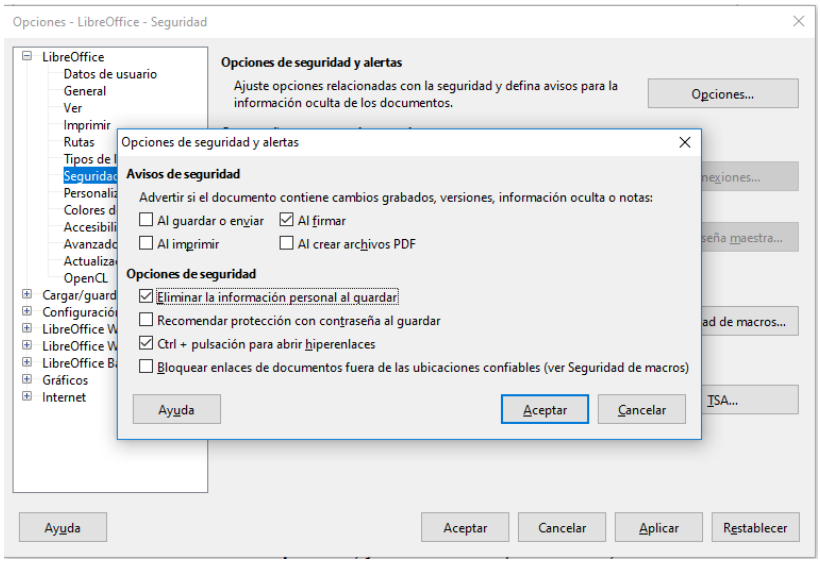
1. Abre LibreOffice e ir Herramientas → Opciones



2. En la ventana que se abrirá, en el menú de la izquierda, **haz click en LibreOffice y después haz click en Seguridad**



3. Haz click en el botón Opciones, y en la ventana que se abrirá, selecciona la casilla Eliminar la información personal al guardar.



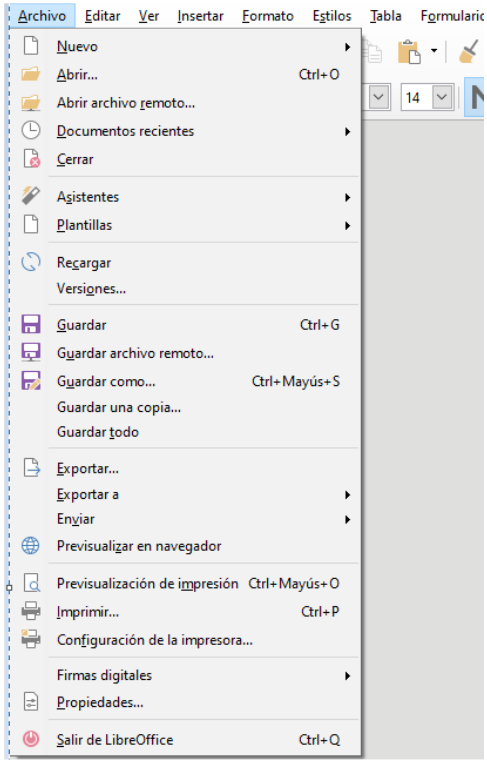
4. Haz click en ***Aceptar***

74. Después de esto, los documentos de LibreOffice se guardarán sin tu información personal.

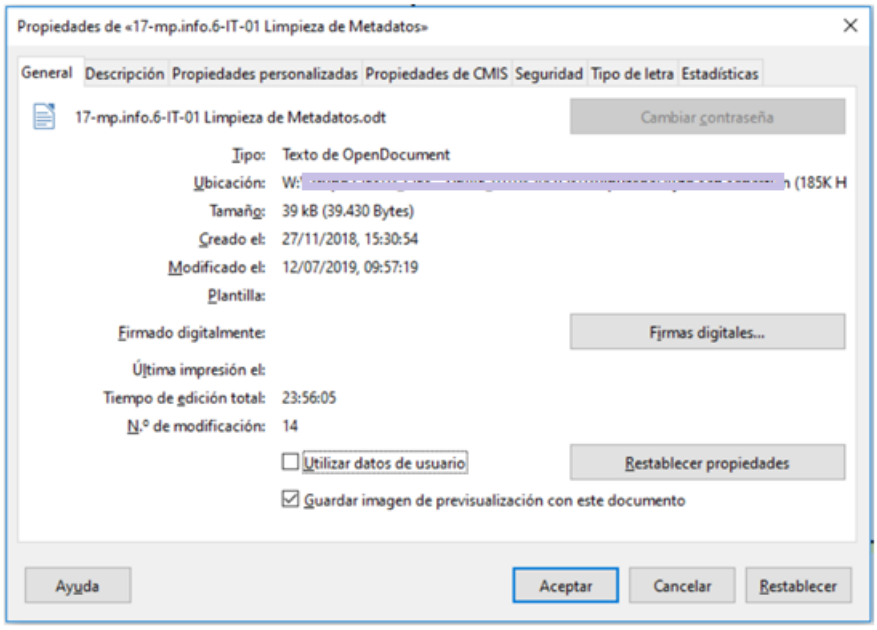
75. METADATOS EN DOCUMENTOS DE LIBREOFFICE

– Eliminar los metadatos en un documento ya creado

1. Ve a Archivo>Propiedades



2. En la pestaña **General,** haz click en el botón **Restablecer propiedades** y desmarca la casilla **Utilizar datos del usuario**.



3. Haz click en **Aceptar**.

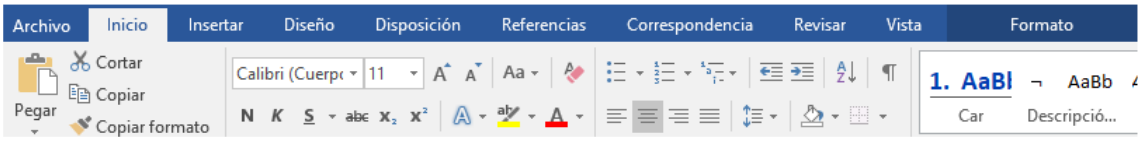
76. METADATOS EN DOCUMENTOS DE MICROSOFT OFFICE

– Evitar que se guarden los metadatos en el documento

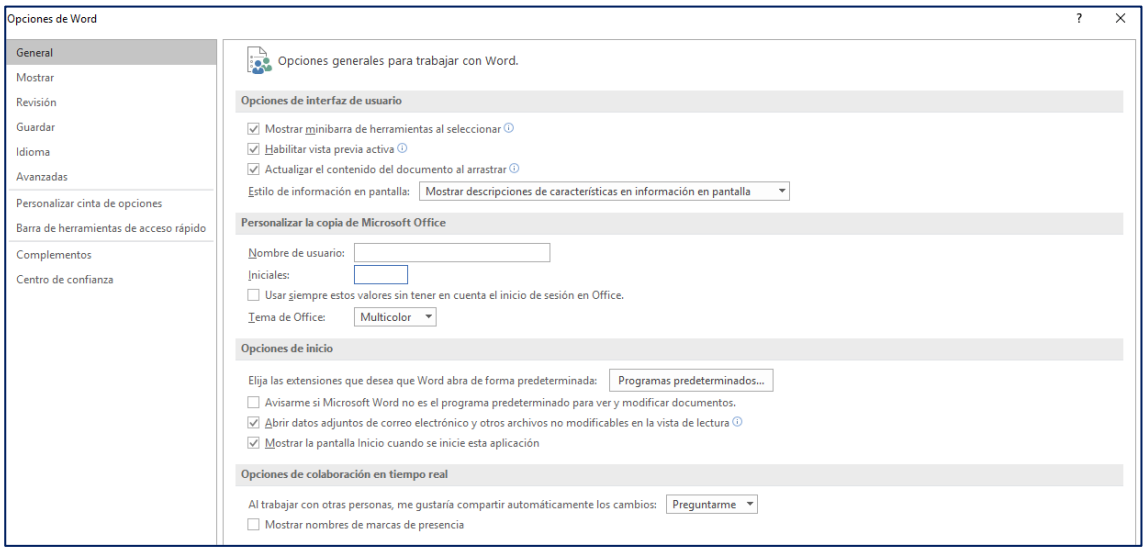
77. A continuación, se establecen las instrucciones a llevar a cabo para evitar que se guarden los metadatos en Microsoft Office versión Microsoft Office Profesional Plus 2016

• Especificar la información personal que aparece en todos los documentos de Office.

1. Abrir Microsoft Office y hacer clic en Archivo y en Opciones



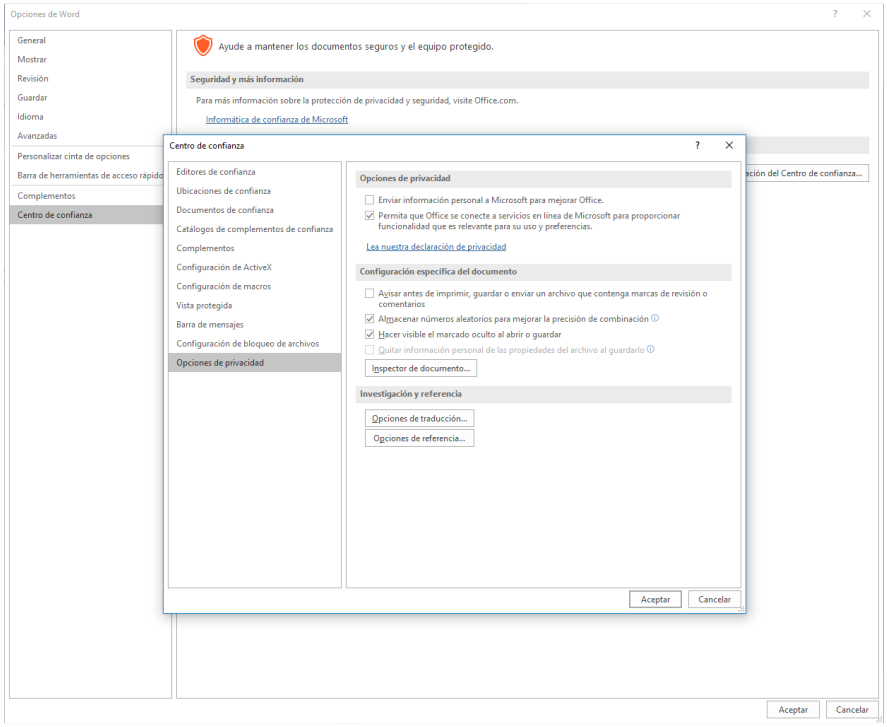
2. En General, en el apartado Personalizar la copia de Microsoft Office, borraremos nuestro nombre e iniciales y remplazaremos por un espacio en blanco en ambos casos.



• No guardar la información personal en un documento de Office

1. Con el archivo abierto, hacer clic en Archivo y a continuación hacer clic en Opciones. Se abrirá la ventana de Opciones de la aplicación, seleccionar Centro de Confianza y pulsar en Configuración del Centro de Confianza. Se abre la ventana de Centro de Confianza.

2. Seleccionar Opciones de privacidad y en el cuadro destinado a Configuración específica del documento aparecerá la opción “Quitar Información personal de las propiedades del archivo al guardarlo”. Esta opción sólo podrá seleccionarse cuando previamente se haya eliminado toda la información personal del documento y hace que cada vez que el documento se guarde, se elimine la información personal.



78. INSPECCIÓN Y BORRADO DE METADATOS E INFORMACIÓN OCULTA

78. Usar el Inspector de documento para buscar y quitar los datos ocultos y la información personal de los documentos de Word.

1. Abra el documento de Word en el que desee buscar datos ocultos o información personal.

2. Haga clic en la pestaña Archivo, luego en Guardar como y a continuación escriba un nombre en el cuadro Nombre de archivo para guardar una copia del documento original.

3. En la copia del documento original, haga clic en la pestaña Archivo y a continuación haga clic en Información.

4. Haga clic en Comprobar si hay problemas y luego haga clic en Inspeccionar documento.

5. En el cuadro de diálogo Inspector de documento, active las casillas para elegir los tipos de contenido oculto que desee que se inspeccionen.

6. Haga clic en Inspeccionar.

7. Revise los resultados de la inspección en el cuadro de diálogo Inspector de documento.

8. Haga clic en la opción Quitar todo situada junto a los resultados de la inspección de los tipos de contenido oculto que desee quitar del documento.

79. IMPORTANTE: Se recomienda usar el Inspector de documento en una copia del documento original, puesto que no siempre se pueden restaurar los datos que quita este inspector.

ÍNDICE