ISGLOBAL
Cultura institucional en materia de protección de datos personales
Un enfoque integrador

Trabajo presentado al *Premio a la Proactividad y Buenas Prácticas en el Cumplimiento del Reglamento General de Protección de Datos y la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales. Modalidad A. Buenas prácticas e iniciativas llevadas a cabo por las empresas, asociaciones y fundaciones del sector privado para el cumplimiento del RGPD y la LOPDGDD.*

TABLA DE CONTENIDOS

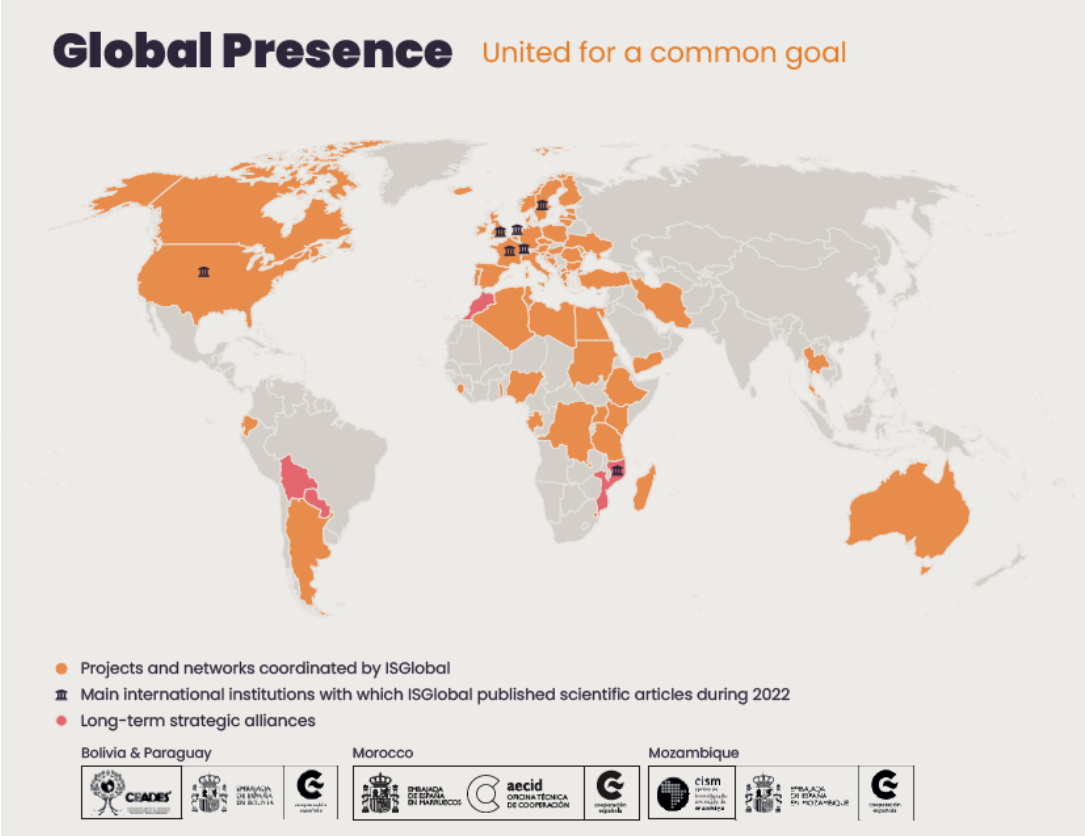
1. ISGLOBAL - LA INSTITUCIÓN

El Instituto de Salud Global Barcelona (ISGlobal) es una institución de vanguardia con capacidad para abordar los retos de la salud pública mundial a través de la investigación e innovación, la traslación y la educación / formación. La misión de ISGlobal es mejorar la salud global y promover la equidad en salud.

ISGlobal es una fundación privada, cuyo principal órgano de gobierno es el Patronato, integrado por la Fundación "la Caixa", el Hospital Clínic, el *Parc de Salut* Mar, la Universidad de Barcelona, la *Universitat* Pompeu Fabra, el Gobierno de España, la Generalitat de Catalunya y el Ayuntamiento de Barcelona. ISGlobal forma parte de CERCA, que agrupa 41 centros de investigación en Cataluña.

Algunos datos sobre ISGlobal

ISGlobal está integrado por más de 540 personas de 46 nacionalidades. Está localizado en Barcelona, en dos Campus (Clínic y Mar) y dispone de unas oficinas en Madrid. Pero su actividad es global, con una presencia en todos los continentes. En ISGlobal trabajamos para reforzar nuestra sólida red con socios en países de renta baja, media y alta, incluido el fortalecimiento de nuestras asociaciones institucionales a largo plazo con la *Fundaçao Manhiça - Centro de Investigaçao em Saúde* de Manhiça (FM-CISM) en Mozambique, así como con Bolivia y Marruecos, en torno a proyectos de alto valor para crear, compartir y aplicar conocimientos.



El enfoque de ISGlobal es multidisciplinar, desde el nivel molecular hasta el poblacional, e incluye disciplinas de las ciencias de la salud, las ciencias de la vida, las ciencias medioambientales, sociales, económicas y climáticas. La investigación de ISGlobal se organiza en torno a cinco programas abarcando las siguientes temáticas: Clima, contaminación atmosférica, naturaleza y salud urbana; Medio ambiente y salud a lo largo de la vida; Infecciones víricas y bacterianas globales; Malaria y enfermedades parasitarias desatendidas; y Salud materna, infantil y reproductiva. Unos 50 investigadores líderes, publican anualmente una media de 600 artículos científicos, y tienen activos aproximadamente unos 250 proyectos financiados a través de convocatorias competitivas, principalmente los programas de financiación europeos (Horizonte 2020 y Horizonte Europa) y otras entidades como *Unitaid*, la Fundación Bill y Melinda Gates, el Ministerio de Ciencia y el Instituto de Salud Carlos III.

En cuanto a la actividad de traslación destaca la implementación de proyectos con un alto componente de innovación, que se traduce en patentes, actualmente 26 activas, la elaboración de informes de traslación y la participación en organismos internacionales como la OMS, y la formación de unos 1000 profesionales cada año.

Los perfiles que integran la institución incluyen a los investigadores, desde los investigadores en formación, pasando por los investigadores postdoctorales hasta los líderes de grupo. Los técnicos que trabajan en los laboratorios, o en la implementación de los proyectos. Los equipos de traslación, en las áreas de innovación, políticas y desarrollo global y formación. Y las personas de soporte, en las unidades de gestión y administración.

El presupuesto anual se sitúa alrededor de los 45M de euros, de los cuales alrededor de un 70-80% es competitivo, mientras que el resto lo aportan los Patronos.

ISGlobal es un centro Severo Ochoa, acreditación de excelencia del Ministerio de Ciencia de España, desde 2019, y tiene el sello de excelencia de Recursos Humanos de la Comisión Europea desde 2015, renovado en 2021 tras la evaluación externa.

2. EL PROCESAMIENTO DE DATOS PERSONALES EN ISGLOBAL

En ISGlobal realizamos diversos tratamientos de datos personales, tal y como describe nuestro Registro de Actividades de Tratamiento, y que incluye:

- **Clientes**: Administración de la base de datos de clientes, facturación y prestación de servicios.
- **Potenciales clientes**: Gestión de la base de datos de potenciales clientes y comunicación precontractual.
- **Empleados**: Gestión de datos laborales de los trabajadores vinculados con la institución.
- **Selección de Personal**: Gestión de la base de datos de candidatos que han presentado solicitudes para puestos vacantes.
- **Formación**: Gestión de la formación interna o externa.
- **Proveedores**: Administración de la base de datos de proveedores, albaranes y servicios prestados.
- **Videovigilancia**: Uso de videovigilancia para garantizar la seguridad y control del entorno y las personas.
- **Investigación**: Manejo de bases de datos especialmente protegidas (por ejemplo, datos de salud) relacionadas con investigaciones como ensayos clínicos o estudios epidemiológicos.
- **Comunicaciones SEPBLAC**: Tratamiento de datos vinculados al cumplimiento de la Ley de prevención del blanqueo de capitales y financiamiento del terrorismo.
- **Comunicación**: Gestión de contactos y solicitantes de información a través de la web u otros medios con fines publicitarios o promocionales.
- **Patronato**: Gestión de la base de datos de los miembros del patronato.
- **Salud Laboral**: Tratamiento de datos de salud de los trabajadores derivados de reconocimientos médicos.
- **Canal de Denuncias**: Investigación y resolución de conductas inapropiadas, especialmente en asuntos de trascendencia penal y cumplimiento normativo según el Protocolo de Gestión, Investigación y Respuesta Externa de Denuncias.
- **Donativos**: Gestión de la base de datos de personas que realizan donativos.

El procesamiento de datos personales en investigación

Podemos afirmar que la **actividad de procesamiento de datos personales más compleja** y la que nos supone un reto mayor en la institución es la **actividad de Investigación**. El procesamiento de datos personales en investigación implica numerosos desafíos y responsabilidades para garantizar el respeto a la privacidad y el cumplimiento de la legislación vigente.

A continuación, incluimos algunos proyectos que ejemplifican esta complejidad, incluyendo el procesamiento de categorías especiales de datos según el Art. 9 del RGPD, la implicación de un número amplio de participantes y poblaciones vulnerables, transferencias de datos dentro del espacio europeo y transferencias internacionales, y el uso de datos previamente recogidos.

Proyecto PRESSURE

PRESSURE tiene como objetivo estudiar los efectos de la contaminación atmosférica y el ruido en la salud mental materna. El proyecto accede a datos ya obtenidos de mujeres embarazadas, aproximadamente 1.200, y sus bebés que conforman la cohorte de nacimiento BISC integrada por participantes del área metropolitana de Barcelona.

El proyecto analiza datos sociodemográficos y de estilo de vida; datos de actividad física y geolocalización; datos sobre la salud mental materna y de la salud del bebé, incluyendo imágenes de resonancia magnética de los bebés.

Proyecto ANTICOV

ANTICOV es un ensayo clínico que pretende responder a la urgente necesidad de identificar tratamientos que puedan utilizarse en el tratamiento precoz de los casos leves a moderados de COVID-19. El objetivo final es evitar oleadas de hospitalizaciones que podrían desbordar los frágiles y sobrecargados sistemas sanitarios de África.

El ensayo clínico se ha llevado a cabo en 19 centros de 13 países africanos por un consorcio formado por 26 organizaciones africanas e instituciones internacionales de investigación y desarrollo.

Se han obtenido datos de aproximadamente 3.000 pacientes, muchos de ellos pertenecientes a poblaciones vulnerables (grupos económicamente desfavorecidos; menores; adultos incapacitados), en un contexto donde las leyes de protección de datos son limitadas.

Proyecto ATHLETE

ATHLETE implica la recogida de nuevos datos en diversas cohortes de nacimiento europeas a través de visitas, cuestionarios, una app que permite registrar la actividad y geolocalización y otros medios. Con ello, será posible generar datos de monitorización de resultados de salud, multi-ómica, exposición química y biomarcadores de efectos en sangre y orina, exposiciones urbanas, contaminación atmosférica, actividad física, así como medir contaminantes clínicos en sangre y orina. La recogida de datos en dos estudios de intervención para analizar el efecto del entorno urbano en los escolares y el efecto de los cosméticos en mujeres.

El estudio ha implicado nuevos datos en aproximadamente 1.300 personas, y el acceso a datos ya recogidos de más de 30.000 personas. ISGlobal es responsable de la gestión de la base de datos centralizada del proyecto.

3. POLÍTICA DE PROTECCIÓN DE DATOS

En ISGlobal disponemos de una **Política en Protección de Datos Personales** (Anexo 1), aprobada en marzo de 2019, que culminó el proceso de adaptación al nuevo reglamento. En mayo de 2021, se aprobó una versión actualizada que incluyó, entre otros, los aspectos relevantes a considerar en situaciones de teletrabajo y movilidad propuestos por la Agencia Española de Protección de Datos a raíz de la pandemia de Covid-19.

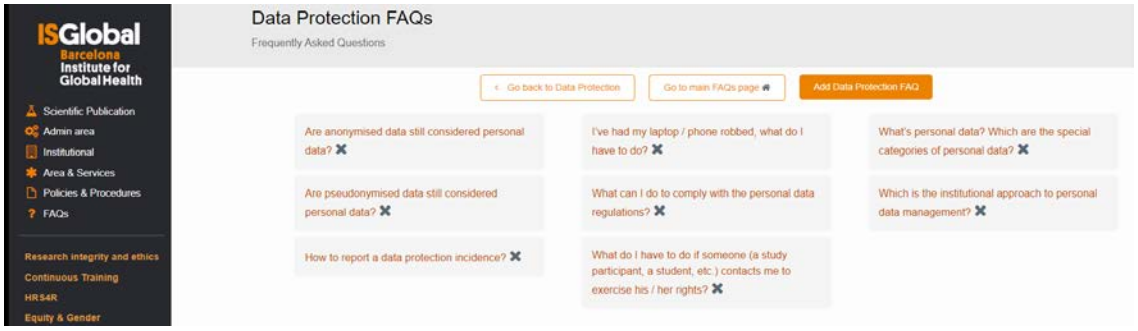
Esta **política se entrega a todo el personal de ISGlobal** en el momento de su incorporación. Aunque la mayoría de las políticas que elaboramos están en inglés por ser el idioma principal del trabajo, en este caso, disponemos de la versión tanto inglesa como castellana, para facilitar la compresión y el conocimiento a todas las personas que trabajan en la institución.

La política cubre **todos los aspectos relevantes para garantizar** que las personas que trabajamos en ISGlobal **cumplamos con la normativa vigente** en materia de protección de datos personales. Se introducen, en primer lugar, los conceptos de protección de datos desde el diseño y por defecto (*privacy by design and by default*), y a continuación se describen los aspectos prácticos sobre recogida, gestión y almacenamiento de datos, los procedimientos generales para salvaguardar la privacidad de los interesados, incluyendo una referencia específica a los procesos de pseudonimización y anonimización y la evaluación de riesgos, el uso compartido y las transferencias de datos. La política informa también sobre los procedimientos internos para comunicar incidencias, y solicitudes de ejercicio de los derechos, así como de las personas a quien contactar y de las opciones de formación.

Uno de los elementos clave es el vínculo entre la **Política de Protección de Datos** y la **Normativa sobre Uso de Recursos y Servicios Informáticos** (Anexo 4). Esta normativa recoge aspectos estrechamente relacionados con la protección de datos, destacando el uso de los equipos informáticos, el acceso a la información y la gestión de las contraseñas, el almacenamiento y las copias de seguridad, el envío de información, el uso y acceso a internet y el uso de correo electrónico. Uno de los puntos de intersección entre ambas políticas es la definición de las medidas de seguridad técnicas y organizativas.

Para facilitar el conocimiento de la normativa, además de la **formación** como elemento clave, tenemos diversos **instrumentos que resumen los aspectos fundamentales de las buenas prácticas en materia de protección de datos** y permiten al personal identificar los elementos clave para garantizar la seguridad de los datos y la privacidad de las personas. Destacamos las **infografías** en las oficinas y otras zonas comunes (Anexo 2) y un apartado en la **intranet** de la institución con **Preguntas Frecuentes** relevantes en materia de protección de datos. De igual modo, durante la emergencia sanitaria por la Covid19, se preparó y distribuyó una infografía y un vídeo específicos sobre los elementos a tener en cuenta en situaciones de teletrabajo y movilidad (Anexo 3).

Preguntas Frecuentes en la intranet



Vídeo Procesamiento de datos personales durante el teletrabajo y en situaciones de movilidad

[Acceso al vídeo]

4. CULTURA INSTITUCIONAL PARA LA PROTECCIÓN DE DATOS PERSONALES

La **protección de datos personales es uno de los pilares** de las instituciones de investigación, especialmente en aquellas centradas en la **investigación biomédica**. Los equipos de investigación necesitan un **asesoramiento continuado y experto** para anticipar y gestionar las necesidades de sus proyectos en materia de protección de datos personales.

En ISGlobal entendemos la protección de datos personales, y las actividades relacionadas, como un **elemento central vinculado a la reputación y al cumplimiento normativo**, pero que, a su vez, trasciende ambos aspectos, y tiene como **prioridad principal** el **respeto por los derechos y libertades de quienes generosamente ceden sus datos más sensibles** (datos de salud) para el avance de la ciencia. El respeto por los derechos y libertades de los participantes no solo es un deber ético, sino que también es crucial para **mantener la confianza y el compromiso de las personas** que colaboran en la investigación.

Nuestro compromiso con ellos es **garantizar su privacidad** y dar respuesta al ejercicio de sus derechos de manera prioritaria. Evidentemente, los datos personales que procesamos en el ejercicio de las otras actividades descritas, son también tratados bajo esta perspectiva.

En ISGlobal, tenemos como objetivo final crear una **cultura institucional** hacia la protección de datos personales, donde **cada miembro de la institución**, independientemente de su cargo y funciones, **incorpore la protección de datos como un elemento esencial en sus actividades diarias**.

Esta cultura institucional se fundamenta sobre **cuatro pilares**:

5. UN ENFOQUE GLOBAL

Un enfoque global de la protección de datos personales, que va más allá de la normativa.

Nuestro enfoque global de la protección de datos personales se fundamenta en una visión que va más allá de cumplir meramente con la normativa aplicable. Reconocemos que la protección de datos es un tema sensible y crítico que involucra no solo aspectos legales, sino también **implicaciones éticas y valores fundamentales de la ciencia abierta**. Por lo tanto, concebimos el procesamiento de datos personales como un componente integral de nuestros proyectos, analizando su relevancia desde una perspectiva más amplia en lugar de tratarlo como una cuestión aislada.

De esta manera, entendemos que la protección de datos (en investigación) es un elemento clave para trabajar con una aproximación a la **ética desde el diseño**. Tal y como describen Borrett y cols. (2017)[1], se trata de "involucrar a los investigadores durante la fase de diseño de la propuesta para que las consideraciones éticas puedan integrarse directamente en la ciencia, en lugar de ser vistas como añadidos a posteriori. Esta propuesta colaborativa de diseño de la investigación da lugar al establecimiento de una **cultura de investigación ética** en lugar de una investigación con supervisión ética". En la misma línea, la Comisión Europea define la ética desde el diseño como la **aplicación**, **desde el inicio del proceso de diseño, de los principios éticos y jurídicos**.

Así pues, la protección de datos se plantea desde el diseño, para garantizar que, desde el planteamiento de la investigación, hasta la recopilación, posterior análisis y almacenamiento de los datos, la **privacidad de las personas participantes esté en el centro** de la toma de decisiones científicas.

[1] DS Borrett, H Sampson, A Cavoukian. Research ethics by design: A collaborative research design proposal. Res Ethics 2017, 13:84-91. https://doi.org/10.1177/1747016116673135

6. LA PROTECCIÓN DE DATOS COMPETE A TODOS LOS MIEMBROS DE LA INSTITUCIÓN

Todos los miembros de ISGlobal contribuyen a garantizar la privacidad de todos: participantes, trabajadores, estudiantes, proveedores, etc.

La protección de datos es una **responsabilidad que recae en todos y cada uno de los miembros** de nuestra institución. Conscientes de la importancia de este tema, en 2017 establecimos un grupo de trabajo interno compuesto por profesionales clave de diversas áreas de la organización. Este grupo incluye a la responsable de Investigación, quien fue designada como delegada de Protección de Datos en 2018, así como al responsable Jurídico, al responsable de Informática y representantes de RRHH, Comunicación, Estadística, Formación y Compras.

Este equipo multidisciplinario, junto con el respaldo de asesores externos especializados, asumió, en su momento, la adaptación al Reglamento General de Protección de Datos (RGPD), y desde 2018, asume la responsabilidad de aplicar el RGPD y la legislación española de protección de datos personales. Además, se encarga de supervisar y hacer cumplir nuestra política interna de protección de datos.

Dentro de este grupo de trabajo, se constituye un **grupo** más restringido, **formado por la delegada de protección de datos, con experiencia en investigación, y los responsables de temas jurídicos y de sistemas de la información**. Este grupo de es el que hace el **seguimiento diario** de la implementación de la normativa y la política interna, en temas como el consentimiento informado de los participantes; la transferencia de datos, desde la revisión de los acuerdos de transferencia hasta los sistemas técnicos para compartir datos; el acceso a datos ya recogidos; el uso de plataformas o herramientas digitales, etc. Este equipo es ampliamente conocido por todos los miembros de la institución y da respuesta a una media de 15-20 cuestiones al mes sobre temas relacionados con el procesamiento de datos personales.

De acuerdo a nuestro planteamiento, **cada miembro de la institución recibe la formación y orientación** necesarias para entender su papel en la protección de datos para salvaguardar la privacidad de los participantes en nuestras investigaciones. Fomentamos una **cultura transversal y colaborativa de concienciación, sensibilización y responsabilidad** en torno a la protección de datos, promoviendo **buenas prácticas y respeto** por la privacidad en todas las actividades relacionadas con la investigación.

Este **enfoque colaborativo** garantiza que la protección de datos sea una prioridad en todas las etapas de nuestros proyectos, desde la recopilación inicial hasta el análisis y la difusión de resultados, e incluyendo también los aspectos de gestión. Con el **compromiso conjunto** de todos los miembros de nuestra institución, aseguramos que nuestros investigadores actúen de manera ética y cumplan con las regulaciones aplicables, protegiendo los derechos y libertades de los participantes en nuestros proyectos que generosamente confían en nosotros sus datos personales.

7. EL SISTEMA DE REPORTE INSTITUCIONAL

La protección de datos como elemento dentro de la gobernanza institucional.

Para garantizar un **sistema de reporte institucional sólido y efectivo,** hemos implementado un sistema de información integral que involucra a diferentes comités y áreas clave dentro de la institución. Este sistema incluye la participación de los Comités de Dirección y Científico, el Comité de Cumplimiento (*Compliance*) y la Administración.

Los miembros del grupo de trabajo interno mencionado anteriormente desempeñan un papel activo en estos órganos de administración y gobierno. Su participación en los Comités de Dirección y Científico asegura que los temas relacionados con la protección de datos estén debidamente considerados en la toma de decisiones estratégicas y científicas de la institución.

Por otro lado, su presencia en el Comité de Cumplimiento garantiza que se realicen **evaluaciones periódicas y exhaustivas del cumplimiento normativo** en materia de protección de datos. Esto incluye revisar y actualizar nuestras políticas internas, procedimientos y prácticas para asegurar que se ajusten a los estándares y regulaciones más recientes.

Además, la participación de los miembros del grupo de trabajo en la Administración permite una comunicación efectiva y una coordinación adecuada entre todas las áreas involucradas en el procesamiento de datos personales.

El sistema de reporte institucional que hemos implementado asegura una **supervisión constante** de nuestras actividades relacionadas con la protección de datos. Esto nos permite identificar y abordar oportunamente cualquier desviación o problema potencial, garantizando un manejo ético, responsable y seguro de los datos personales de procesamos, incluyendo la información de los participantes en nuestras investigaciones, y también de los datos que procesamos en el contexto de otras actividades (comunicación, formación, recursos humanos, etc.).

8. FORMACIÓN Y HERRAMIENTAS

De la teoría a la práctica: crear una cultura de cumplimiento a través de la formación continua y la puesta a disposición de herramientas adecuadas.

a. Formación, formación y más formación

Si hay un elemento clave y fundamental para crear cultura en materia de protección de datos es la **formación**. La formación **continua y adaptada a las necesidades de los proyectos y los diversos colectivos** de la institución. En ISGlobal entendemos y planificamos las diferentes actividades de formación más allá de la mera transmisión de conceptos, definiciones y normativas. Se trata de **sensibilizar**, de **generar compromiso** y **responsabilidad compartida** en todo lo que compete a la protección de los datos personales que procesamos en la institución.

Oferta formativa en materia de protección de datos personales

ISGlobal dispone de un **programa de formación interno** que abarca muchos y diversos temas, incluyendo tanto temas organizativos y de desarrollo profesional (por ejemplo, formación en liderazgo o resolución de conflictos) como temas técnicos (por ejemplo, análisis estadístico o sistemas de información geográfica). La **formación en materia de materia de protección de datos personales** se incluye dentro del programa de formación interno de la institución, lo que nos permite coordinar los diferentes colectivos implicados y llegar a todas las personas, fijar formaciones anuales para garantizar que se dispone de los conocimientos necesarios de forma actualizada, y acceder a oportunidades de formación externa.

A continuación, incluimos una descripción de las diferentes actividades formativas que realizamos en materia de protección de datos personales y temas relacionados:

Sesiones *ad hoc* con los grupos de investigación en el marco de proyectos específicos

Los proyectos que desarrollamos en la institución tienen necesidades muy concretas en relación al procesamiento de datos personales. Como se ha descrito con anterioridad, algunos proyectos se basan en el procesamiento de datos ya recogidos, otros implican la obtención de datos prospectivos en poblaciones muy diferentes (menores, adultos sanos, adultos con patologías, ciudadanos, profesionales, en países europeos o países en desarrollo) y utilizando técnicas muy diversas (encuestas en papel u online, *focus groups*, sistemas de geolocalización con dispositivos móviles, cámaras, etc.).

Para dar una mejor respuesta a los equipos de investigación, se organizan sesiones *ad hoc* donde revisan los conceptos generales de protección de datos (normativa, definición de dato personal y categorías especiales, anonimización / pseudonimización, transferencias, etc.), la política, procedimientos y herramientas institucionales y de forma específica las implicaciones que el propio proyecto supone, de manera que su implementación se ajuste a la normativa y a las buenas prácticas.

Normalmente, organizamos entre 4 y 5 formaciones anuales, con la implicación de unas 50 personas integrantes de equipos de investigación. Un ejemplo del material utilizado puede verse en el Anexo 5.

Sesiones periódicas para la administración y personal de soporte

Una parte importante de la institución trabaja en la administración y otras áreas de soporte. Para estas personas se organizan sesiones periódicas, semestrales o anuales según el colectivo y los datos que procesa. En estas sesiones, se revisan los conceptos generales, y, especialmente, se actualiza sobre la política, procedimientos y herramientas institucionales. Llegamos a unas 75 personas anualmente.

Curso sobre Integridad en la Investigación y Ética

Este es un curso obligatorio para todos los investigadores predoctorales, postdoctorales y líderes de grupo juniors, y abierto a cualquier otro perfil de la institución. Incluye diversas sesiones sobre integridad en la investigación, aspectos éticos, y por supuesto, una sesión específica sobre protección de datos personales, donde se informa con detalle sobre la política, procedimientos y herramientas institucionales, y otra sesión sobre gestión de datos. El curso tiene dos ediciones anuales (primavera y otoño) para garantizar que todas las nuevas incorporaciones pueden acceder. Se forman aproximadamente unas 60 personas cada año.

Curso de técnicas anonimización / pseudonimización para el equipo de Estadística y Gestión de Datos

Este es un curso dirigido a estadísticos y gestores de datos (Anexo 6). La primera edición de este curso se realizó en marzo de 2021, y permitió generar un repositorio de material (guías, modelos, etc.) para todo el colectivo. Asistieron más de 30 personas.

Actualmente estamos en proceso de organización de la segunda edición para dar cobertura a las nuevas incorporaciones. Está planificado como resultado del curso, crear un foro interno que permita el intercambio de buenas prácticas y metodologías entre los profesionales estadísticos y de gestión de datos que se integran en los diferentes equipos y proyectos.

Curso de Ciberseguridad

El curso de ciberseguridad es un curso online obligatorio para todos los miembros de ISGlobal, independientemente de su posición y/o actividad. Desde su implementación en diciembre de 2021, todo el personal contratado en ese momento y todas las nuevas incorporaciones deben realizar el curso durante el primer mes tras su incorporación. En caso contrario, se bloquea su acceso a los servicios de red de la institución (servidores, correo electrónico corporativo, VPN, intranet). Disponemos también de un decálogo sobre ciberseguridad que se revisa a lo largo del curso (Anexo 7).

Los temas que se tratan incluyen: ¿Qué es la Ciberseguridad?; Tipos de ataques y de amenazas; Las personas figuras claves en la ciberseguridad; ¿Qué información debe protegerse?; La información es el principal activo de la empresa; Ciclo de vida de la información; Buenas prácticas en Protección de la Información; Cómo gestionar un incidente / Incidentes más comunes; ¿Qué normativa debo cumplir?; Decálogo de Seguridad de ISGlobal.

En 2022, se formaron 480 personas (sobre un total de 559 convocadas, 86%), en 4 convocatorias consecutivas. En 2023, con un acceso continuado al curso, se han formado 174 personas.

Otras actividades formativas

Adicionalmente a las formaciones más concretas, aprovechamos otras ocasiones para incidir en el tema de la protección de datos personales. Por ejemplo, la institución organiza una reunión anual con cada uno de los colectivos para repasar nuevas políticas, procedimientos, etc. de interés, donde siempre incluimos una actualización en materia de protección de datos. De igual modo, si se organizan sesiones de Preguntas Frecuentes, también se incluyen los aspectos de protección de datos.

Y siempre deseamos a todos los miembros de la institución un feliz día en la celebración del día europeo de protección de datos el 28 enero.

a. Herramientas

Es nuestro deber como institución facilitar las herramientas necesarias para que las diferentes personas que integran la institución puedan cumplir con los requerimientos en materia de protección de datos. Unas herramientas claras, accesibles, conocidas y constantemente actualizadas son esenciales para garantizar el correcto manejo y resguardo de la información que manejamos.

La Política de Protección de Datos Personales (ver Sección 3) es la base sobre la cual se desarrollan e implementan las diferentes herramientas:

Soporte continuado

Nuestro compromiso radica en brindar un **soporte continuado en materia de protección de datos.** A través de la dirección de correos: lopd@isglobal.org, estamos siempre disponibles para atender cualquier consulta o inquietud relacionada con la protección de datos, asegurando una respuesta rápida y efectiva. Llevamos a cabo un análisis de las necesidades específicas de cada proyecto, adoptando una visión colaborativa que involucre a todos los miembros del equipo. Los investigadores saben que formamos parte de su equipo para dar respuesta a los aspectos de protección de datos de sus proyectos.

Nos comprometemos también a mantener informados a todos los miembros de la institución a través de correos electrónicos (Anexo 8) y noticias en la intranet.

Procedimientos específicos

Desarrollamos **procedimientos específicos**, para poder responder de manera ágil ante determinadas situaciones. Tenemos un protocolo de actuación en caso de robo o pérdida de equipos institucionales (ordenadores portátiles, teléfono móvil) (Anexo 9). Este protocolo se revisa en las diferentes actividades formativas descritas, y se comunica de forma periódica en la intranet institucional. De igual manera, se informa a todas las personas sobre los derechos en materia de protección de datos de acuerdo al RGPD y cómo proceder en caso de ser contactado por un o una participante que desee ejercerlos.

Modelos y plantillas

Disponemos de una serie de **documentos modelo y plantillas** accesibles a través de la intranet del centro para dar respuesta a los diferentes tratamientos que realizamos.
Destacamos el modelo de Hoja de Información y Consentimiento Informado (Anexo 10) para participantes en los proyectos de investigación. Este documento, que ha sido validado por el comité de ética que nos supervisa, incluye una cláusula específica de protección de datos que cubre toda la información que deben recibir los participantes de acuerdo al Art 13. RGPD.

Las diferentes áreas (Formación, RRHH, Compras, Comunicación) disponen también de modelos y plantillas predeterminadas que se adaptan según las características del proyecto / actividad de tratamiento de datos, entre ellos: contrato de encargado de tratamiento o contrato de corresponsabilidad en el tratamiento de datos, acuerdo para transferencia de datos, evaluación de impacto (ver Sección 8b), cesión de imágenes para menores y adultos, confidencialidad de los estudiantes, información y compromiso de los trabajadores, privacidad en las ofertas de trabajo y matriculación en cursos externos, política de privacidad de los sitios web.

Herramientas informáticas

Entre las diferentes herramientas informáticas de las que disponemos (ver Normativa sobre Uso de Recursos y Servicios Informáticos en el Anexo 4), queremos destacar el **módulo de reporte y seguimiento que tenemos en la intranet para comunicar cualquier posible incidencia** en materia de protección de datos, por ejemplo, el robo de un equipo, la pérdida de documentación, la recepción por correo de datos personales, etc. Todas las personas de ISGlobal son informadas del funcionamiento de esta herramienta que permite hacer un seguimiento adecuado de cualquier incidencia, identificar si se trata de una brecha de seguridad que debiera ser comunicada a la Agencia, y determinar qué medidas / acciones deben implementarse. Otras herramientas destacadas, son la **VPN** que permite la conexión remota segura y el acceso protegido y cifrado a los servicios de red internos y repositorios de datos ubicados en los servidores internos, y el **Espacio Privado** (*Private Cloud*) que permite compartir y transferir datos de forma segura y cifrada (protocolo HTPPS), ya que se trata de un entorno de trabajo privado espacio debidamente protegido seguro con acceso restringido con credenciales individuales que permite el envío y recepción de datos / información cifrada entre los colaboradores externos.

b. La evaluación del riesgo

El **Mapa de Riesgos de ISGlobal se configura como una herramienta interna de gestión** cuya finalidad es identificar las actividades, procesos o actuaciones de ISGlobal que se encuentran expuestos a riesgos o amenazas, cuantificando la probabilidad de que esos eventos sucedan y midiendo el daño potencial asociado a su ocurrencia. El Mapa de Riesgos tiene asimismo vocación de servir de marco de referencia a la hora de **definir estrategias, políticas o actuaciones** en la organización -en particular, las destinadas a **disipar esos focos de riesgo**-, así como también de los **mecanismos de supervisión, monitorización y control interno** de las actividades o procesos clave.

En el "catálogo de riesgos", se han identificado las siguientes categorías de riesgos: estratégicos, operativos, financieros, de cumplimiento y reputacionales. Dentro de los riesgos de cumplimiento tenemos un riesgo directamente relacionado con la protección de los datos personales: *"Brechas en la seguridad de los sistemas que puedan tener un impacto en la continuidad operativa de la institución y/o en el acceso no autorizado a datos de carácter personal o información confidencial.".*

Y dentro de los riegos operativos, el presente riesgo *"Menoscabo de la integridad o pérdida de los datos por causas o factores internos/externos."* también implica elementos de protección de datos personales.

El hecho de incluir estos riesgos como parte del Mapa de Riesgos institucional, nos permite **establecer las políticas necesarias** para mitigar su posible impacto en caso de ocurrencia, y **abordarlos desde una perspectiva institucional** como parte de la gobernanza de la institución, como se ha descrito en la Sección 7.

Evaluación de Impacto relativa a la Protección de Datos

Nuestro primer planteamiento en la evaluación de los riesgos asociados a la protección de datos personales fue realizar, en 2019, dos evaluaciones de impacto relativas a la protección de datos (EIPD) desde una perspectiva institucional en las áreas de Investigación y de Comunicación. Estas evaluaciones de impacto se realizaron conjuntamente con asesores externos.

Estas EIPDs sirvieron de base para identificar los principales riesgos que afectan al conjunto de la actividad investigadora y de comunicación y proponer las medidas que permitan reducirlos.

En 2021, se realizó una EIPD en el ámbito del tratamiento de datos necesario para cumplir con las obligaciones relativas a la prevención el área del blanqueo de Capitales y de la financiación del terrorismo internacional.

Las medidas propuestas en estas evaluaciones se comparten con el resto de integrantes del grupo de trabajo en protección de datos para realizar el seguimiento de su implementación, junto con las medidas derivadas de las auditorías externas (ver Sección 8c).

A partir de la EIPD institucional sobre la actividad investigadora de evalúan las actividades de procesamiento de datos en los diferentes proyectos que se lleva a cabo en la institución y se determina la necesidad de realizar una **evaluación específica centrada en la actividad del proyecto** cuando ésta no queda cubierta por la evaluación institucional. Para ello, disponemos de un modelo que los investigadores cumplimentan con la ayuda de la delegada de protección de datos, donde se revisa y analiza en detalle el procesamiento de datos personales, se identifican los riesgos y se describen las medidas a implementar para su reducción. Este documento se comparte con el resto de integrantes del grupo de investigación.

c. Auditorías externas

Para garantizar que nuestros procesos cumplen con la normativa vigente e identificar áreas de mejora en nuestras actividades de protección de datos, realizamos **auditorías externas periódicas en materia de protección de datos personales.** Desde la implementación del RGPD, hemos realizado una auditoria en octubre de 2020, y tenemos programada la nueva auditoría en noviembre de 2023.

Concebimos estas **auditorías**, no tan sólo como una oportunidad de mejora, sino también como una **oportunidad de sensibilización y formación** para las personas de la institución. Involucramos a personas de diferentes perfiles, tales como investigadores, técnicos, personal de dirección, etc. De esta manera ampliamos la cobertura de las actividades de procesamiento a revisar y generamos concienciación sobre la relevancia de garantizar la privacidad en los procesos que les implican. Como ejemplo, podemos mencionar las actividades del Grupo de Género y Equidad, el procedimiento de acoso laboral, el procedimiento de gestión de posibles casos de mala praxis científica, etc.

Mencionar también, que recientemente hemos realizado una **auditoría de vulnerabilidades externas (AVEX) en el ámbito de la ciberseguridad**, que nos ha permitido identificar, evaluar y adoptar medidas para corregir posibles brechas de seguridad en nuestros sistemas de red, diversas páginas y aplicaciones web.

9. MÁS ALLÁ DE LA INSTITUCIÓN

Finalmente, queremos destacar **nuestro rol en promover la sensibilización y formación** en materia de datos personales **más allá de nuestra institución.**

Los aspectos éticos y, dentro de ellos la protección de los datos personales, se incluyen en el **Máster de Salud Global y el Máster de Investigación Clínica** que coordinamos desde ISGlobal. De esta manera, todos los alumnos que atienden a estos másteres participan en una sesión en la que se revisan los conceptos clave relacionados con la protección de datos personales y se discuten las implicaciones del procesamiento de datos personales en la investigación.

Somos también coordinadores de la **Red Europea de Ética e Integridad** (ERION) dentro de la Asociación Europea de Gestores de Investigación y Administración (EARMA). Esta red participada por gestores de ciencia de diversos países europeos permite el **debate, el aprendizaje y el intercambio de buenas prácticas** en diversos temas, uno de ellos la implementación del RGPD. Como ejemplo, incluimos el poster que presentamos en la última reunión de EARMA (2023) sobre la cultura institucional en protección de datos (Anexo 11).

Como último, queremos destacar la participación en **actividades de formación internacionales**, especialmente con nuestros socios en países de renta media-baja. Destacamos los cursos ofrecidos en el marco del Proyecto PamAfrica en septiembre de 2022, donde se impartió una sesión sobre ética y protección de datos personales a más de 50 personas, investigadores y gestores de diferentes centros de investigación e instituciones académicas de África. Y las sesiones sobre ética y protección de datos dentro del Curso de Capacitación en *Data Science*. Dichas sesiones se impartieron a más de 150 investigadores y gestores de datos de Bolivia y Paraguay, en octubre y diciembre de 2022 respectivamente.

10. MATERIAL ANEXO

1- Política de Protección de Datos personales
2- Normativa sobre Uso de Recursos y Servicios Informáticos
3- Infografía sobre protección de datos para oficinas y zonas comunes
4- Infografía sobre procesamiento de datos personales en situaciones de teletrabajo y movilidad
5- Ejemplo de materia utilizado en las sesiones *ad hoc* sobre protección de datos
6- Temario curso sobre técnicas de anonimización / pseudonimización
7- Decálogo de ciberseguridad
8- Ejemplo de correo electrónico para actualizar a todo el personal sobre temas de protección de datos personales
9- Protocolo de actuación ante el robo de equipo institucional
10- Modelo para la preparación de una Hoja de Información y Consentimiento para un proyecto de investigación
11- Poster presentado a la reunión de EARMA en abril de 2023 sobre la Cultura institucional en materia de protección de datos

ISGlobal

Política de Protección de Datos Personales

Barcelona, 05 de Mayo de 2021

Política de protección de datos personales	Fecha de aprobación 05 Mayo 2021	Autor/a Delegada de protección de datos	Revisado por Miembros del grupo de trabajo en protección de datos (WG LOPD), M. Benet (estadístico), M. Guxens (Assistant RP) Comisión de Equidad y Género Coordinadora de Calidad	Aprobado por Comité de Dirección

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

Tabla de contenido

Política de protección de datos personales	Fecha de aprobación 05 Mayo 2021	Autor/a Delegada de protección de datos	Revisado por Miembros del grupo de trabajo en protección de datos (WG LOPD), M. Benet (estadístico), M. Guxens (Assistant RP) Comisión de Equidad y Género Coordinadora de Calidad	Aprobado por Comité de Dirección

1. OBJETIVO

- Facilitar unas directrices sobre la protección de datos personales que abarquen desde la recogida hasta la conservación de los datos, pasando por la gestión (incluyendo su uso compartido y transferencia).
- Garantizar que en ISGlobal los datos personales se tratan y conservan de conformidad con lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (el RGPD), Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y la Ley 14/2007 de Investigación Biomédica.

2. ALCANCE

- La presente política será aplicable a todo el personal de ISGlobal que gestione datos personales, independientemente del área o departamento y de la procedencia de tales datos (Investigación, Formación, Análisis y Desarrollo Global, Administración).

3. DEFINICIONES Y SIGLAS

CONCEPTOS CLAVE: A continuación, se incluyen únicamente los conceptos clave. Para obtener una lista completa de definiciones, véase el artículo 4 del RGPD.

- **Datos personales** significa **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 de dicha persona.
    - La interconexión de determinados datos podría llevarnos asimismo a identificar a una persona, por ejemplo, combinando una enfermedad poco común con el lugar de nacimiento, la edad y el sexo.
    - La geolocalización y el geoseguimiento implican el tratamiento de datos personales.
    - La voz y las imágenes también son datos personales.
- **Las categorías especiales de datos personales** (anteriormente conocidos como «datos sensibles») comprenden «datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de **datos genéticos**, **datos biométricos** dirigidos a identificar de manera unívoca a una persona física, datos relativos a la **salud** o datos relativos a la vida sexual o la orientación sexuales de una persona física» (artículo 9 (1) del RGPD).
- **Tratamiento de datos** significa cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro,

Política de protección de datos personales	Fecha de aprobación 05 Mayo 2021	Autor/a Delegada de protección de datos	Revisado por Miembros del grupo de trabajo en protección de datos (WG LOPD), M. Benet (estadístico), M. Guxens (Assistant RP) Comisión de Equidad y Género Coordinadora de Calidad	Aprobado por Comité de Dirección

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;

SIGLAS:

- DPD: Delegada de protección de datos
- CCD: Contrato de Cesión de Datos
- RGPD: Reglamento General de Protección de Datos
- CCM: Contrato de Cesión de Muestras

4. DESPLIEGUE DE LA POLÍTICA

a) Protección de datos desde el diseño y por defecto de conformidad con el RGPD (artículo 25)

(https://gdpr-info.eu/art-25-gdpr/)

- La protección de datos se efectuará «desde el diseño» y «por defecto».
  - Desde el diseño: se aplicarán medidas técnicas y organizativas para proteger los datos personales, desde las **primeras etapas del diseño** de las operaciones de tratamiento, de modo que se salvaguarden los principios de privacidad y protección de los datos desde el principio.
  - Por defecto: **solo serán 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.

b) Recogida, gestión y conservación de datos personales

i. Procedimientos generales para salvaguardar la privacidad de los interesados/das

- **Deberá obtenerse el consentimiento explícito** del interesado para tratar sus datos personales. Todas las actividades de tratamiento requieren la obtención del consentimiento explícito mediante una cláusula específica sobre la protección de datos personales, en la que se informe al interesado/a de cómo se tratarán y conservarán sus datos, de cuál es el fin de investigación, de los datos de contacto de la DPD y de los derechos del interesado/a. Véanse las cláusulas específicas de tratamiento en el siguiente Anexo.
- Deberá aplicarse el principio de **minimización de datos**. Lo anterior significa que solo se recogerán, tratarán y conservarán los datos que sean necesarios en función de los objetivos perseguidos y proporcionales a estos.
- La **seudonimización** se aplicará como medida general, lo que significa que todo el material recopilado en el marco del proyecto (cuestionarios, informes, muestras biológicas, imágenes médicas, etc.) se identificará mediante un código, y en ningún caso se consignarán el nombre propio y/u otro dato de carácter personal que permita la identificación del interesado/a. Este identificador único permitirá vincular todos los datos esenciales necesarios para el estudio de investigación. El fichero de claves maestras que vincula los códigos de los

Política de protección de datos personales	Fecha de aprobación 05 Mayo 2021	Autor/a Delegada de protección de datos	Revisado por Miembros del grupo de trabajo en protección de datos (WG LOPD), M. Benet (estadístico), M. Guxens (Assistant RP) Comisión de Equidad y Género Coordinadora de Calidad	Aprobado por Comité de Dirección

estudios de investigación del centro con los identificadores personales se guardará en un archivo de acceso restringido protegido mediante contraseña. Siempre que sea posible, se recurrirá a la anonimización.

- Todos los ficheros que contengan datos personales (o la clave de datos seudonimizados) deberán guardarse en **archivos cifrados y protegidos mediante contraseña**, de acceso restringido, en los servidores de la entidad. El acceso a tales archivos estará limitado a personal autorizado (los miembros de un determinado departamento o proyecto) y deberá ser objeto de seguimiento. No deberán guardarse archivos que contengan datos personales en los ordenadores de los usuarios/as.
- En el caso del **seguimiento realizado a participantes** mediante técnicas de geolocalización, los datos resultantes deberán conservarse por separado con respecto de otros datos del participante (sobre la salud, etc.).
- Los resultados de **estudios de investigación reportados** formarán parte de análisis de **datos agregados**. No deberá asociarse el nombre de ningún particular con ningún informe de investigación publicado o no.
- **Comunicación masiva.** En caso de que necesite enviar información a una cantidad elevada de interesados/as, póngase en contacto con SRI, puesto que tal acción deberá realizarse a través de una plataforma especial para evitar problemas relacionados con el tratamiento de contenido no deseado.

ii. Uso compartido de los datos y transferencia internacional de datos personales

- Como norma general, **los datos personales no deberán ser objeto de transferencia**, salvo en los casos previstos por la ley.
- Aquellos datos que se hayan anonimizado y/o seudonimizado por completo podrán transferirse a terceros independientemente del país. Para ello, se requerirá un CCD (más adelante, se incluye más información al respecto).
- En todo caso, si es necesario transferir datos personales, deberá informarse debidamente a los interesados (por ejemplo, los participantes de un proyecto, estudiantes, etc.) y deberán adoptarse medidas que garanticen la protección de los datos personales. La transferencia se realizará de conformidad con la legislación vigente:
    - Las transferencias entre los Estados miembros de la UE están permitidas en virtud del RGPD.
    - La transferencia de datos personales a un tercer país o una organización internacional podrá efectuarse cuando la Comisión haya decidido que dicho tercer país, territorio o sector o sectores específicos de dicho tercer país, o la organización internacional en cuestión, ofrece un nivel de protección de datos adecuado.

  (AEPD Transferencias internacionales; Decisiones de adecuación de la CE)
- Antes de transferir datos personales a otra organización, póngase en contacto con su DPD (lopd@isglobal.org) o con la responsable de Gestión Paralegal (contracts.management@isglobal.org).
- Antes de compartir datos o muestras biológicas, deberá firmarse un Contrato de Cesión de Datos (CCD) o un Contrato de Cesión de Muestras (CCM). Póngase en

Política de protección de datos personales	Fecha de aprobación 05 Mayo 2021	Autor/a Delegada de protección de datos	Revisado por Miembros del grupo de trabajo en protección de datos (WG LOPD), M. Benet (estadístico), M. Guxens (Assistant RP) Comisión de Equidad y Género Coordinadora de Calidad	Aprobado por Comité de Dirección

contacto con la responsable de Gestión Paralegal (contracts.management@isglobal.org), quien le facilitará los modelos institucionales y le orientará a lo largo de todo el proceso.

- La transferencia de datos personales deberá efectuarse mediante protocolos seguros de transferencia de archivos (por ejemplo, SFTP, HTTPS, sistemas privados de administración en la nube). No está permitido el uso del correo electrónico. Póngase en contacto con el equipo de SRI si necesita ayuda a lo largo del proceso (sri.tic@isglobal.org).

c) Relación con nuestra política interna sobre el uso de recursos y servicios informáticos

- ISGlobal ha implementado una **normativa pormenorizada respecto del uso de recursos y servicios informáticos** (ISG-IT-POL-UseComputerResouresITServices), de conformidad con la cual todo el personal de ISGlobal deberá firmar una declaración relativa al uso de tales recursos y servicios (véase el Anexo 3 de la normativa anteriormente mencionada). Le rogamos que lea el documento detenidamente y que se ponga en contacto con el equipo de SRI en caso de dudas (sri.tic@isglobal.org).
- A continuación, se incluye una síntesis de las directrices pertinentes en materia de recursos informáticos y gestión de datos personales:
  - Para acceder a los servicios de la red deberá disponerse de un nombre de usuario y una contraseña intransferibles.
  - No deberán enviarse datos personales por correo electrónico u otras herramientas de comunicación en abierto/externas tales como WhatsApp, Dropbox, Google Drive personal, o cualquier otra aplicación móvil no corporativa.
  - No deberán utilizarse conexiones wifi públicas/externas.
  - No deberán almacenarse datos personales en el ordenador del usuario; todos los archivos que contengan datos personales deberán almacenarse en el servidor.
  - Se recomienda encarecidamente no recibir/enviar faxes que contengan datos personales. En caso de que sea necesario, el empleado/a de ISGlobal que reciba o envíe un fax deberá asegurarse de que su destino es seguro.
  - Los usuarios/as no deberán dejar sus ordenadores desatendidos cuando estén trabajando con datos personales. En caso de que sea necesario, deberá bloquearse el acceso al ordenador (Ctrl+Alt+Supr).
  - Deberá prestarse especial atención a los objetos incrustados o vinculados, puesto que el archivo original podría contener datos personales.
  - Deberá extremarse la precaución cuando se utilicen dispositivos portátiles (memorias USB, discos duros portátiles, otros dispositivos de almacenamiento extraíbles). Se recomienda encarecidamente proteger el acceso a los ficheros mediante contraseña. No deberán almacenarse o transportarse datos personales en dispositivos de almacenamiento extraíbles y tampoco en ordenadores de uso doméstico.

Política de protección de datos personales	Fecha de aprobación 05 Mayo 2021	Autor/a Delegada de protección de datos	Revisado por Miembros del grupo de trabajo en protección de datos (WG LOPD), M. Benet (estadístico), M. Guxens (Assistant RP) Comisión de Equidad y Género Coordinadora de Calidad	Aprobado por Comité de Dirección

- Se realizan copias de seguridad de todos los archivos guardados en el sistema de información y en los ordenadores de los usuarios/as con una frecuencia diaria y semanal, respectivamente.
- Deberá vaciarse la papelera de reciclaje del ordenador tras eliminar cualquier documento que contenga datos personales.
- En caso de que un ordenador pase a ser de otro usuario/a, deberá ser previamente formateado.
- Se evitará imprimir documentos que contengan datos personales. En caso de que ello sea necesario (información de recursos humanos, formularios de consentimiento), no deberán dejarse tales documentos desatendidos en la impresora y deberán guardarse bajo llave. En caso de que sea preciso destruir un documento que contenga datos personales, deberá utilizarse alguna de las destructoras de papel / contenedores de papel, que se encuentran disponibles en:
  - Campus Clínic: en la 4.ª planta (cerca de la fotocopiadora) y la 6.ª planta (cerca del despacho de RR. HH.).
  - Campus Mar: en la 1.ª planta cerca de la fotocopiadora, y en Hipàtia cerca del despacho de RR. HH.

d) Nota sobre el proceso de seudonimización y anonimización

– Trabajar con grandes conjuntos de datos representa un reto para el proceso de seudonimización/anonimización. Los siguientes documentos analizan la eficacia y los límites de las técnicas de anonimización existentes en la actualidad y ofrecen recomendaciones para aplicar dichas técnicas:
https://www.pdpjournals.com/docs/88197.pdf
https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf

e) El registro de las actividades de tratamiento de ISGlobal

– De conformidad con lo dispuesto en el artículo 30 del RGPD, ISGlobal dispone de un registro interno de las actividades de tratamiento que comprende todas las actividades relacionadas con el tratamiento de datos personales que realizamos. La DPD se encarga de supervisar dicho registro y de actualizarlo si procede. Las actividades de tratamiento son: clientes, canal de comunicación de reclamaciones, empleados, selección de personal, proveedores, salud laboral, clientes potenciales, investigación, comunicaciones ante el SEPBLAC (relacionadas con casos de fraude), formación para el Patronato, videovigilancia.

f) Evaluación de impacto relativa a la protección de datos

– De conformidad con lo dispuesto en el artículo 35 del RGPD, deberá realizarse una evaluación de impacto relativa a la protección de datos (EIPD) si se da por lo menos alguna de las siguientes circunstancias:
  1. evaluación sistemática y exhaustiva de aspectos personales de una persona física, incluida la elaboración de perfiles;
  2. tratamiento a gran escala de datos sensibles,

Política de protección de datos personales	Fecha de aprobación 05 Mayo 2021	Autor/a Delegada de protección de datos	Revisado por Miembros del grupo de trabajo en protección de datos (WG LOPD), M. Benet (estadístico), M. Guxens (Assistant RP) Comisión de Equidad y Género Coordinadora de Calidad	Aprobado por Comité de Dirección

3. observación sistemática a gran escala de zonas de acceso público.

– Si un proyecto determinado cumple alguna de las circunstancias anteriores, se llevará a cabo una EIPD, que incluirá los apartados especificados en el artículo 35, punto 7, del RGPD (Anexo)

g) Comunicación de incidencias

– Quien detecte una incidencia en relación con la gestión de datos personales, deberá rellenar el formulario de comunicación de incidencias correspondiente (véase el siguiente Anexo) e informar de ello a la DPD (lopd@isglobal.org).
– Algunos ejemplos de incidencias son:
  - Robo/extravío de un portátil o un móvil.
  - Extravío de consentimientos informados ya firmados.
  - Recepción de datos personales a través del correo electrónico.

h) Derechos del interesado (derechos ARCO)

– Todos los interesados/as gozan de derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad de los datos y oposición al tratamiento de los datos, de conformidad con las disposiciones en materia de protección de datos (artículos del 15 al 21 del RGPD).
– Si tiene constancia de que un interesado/a desea ejercer sus derechos, póngase en contacto con la DPD lo antes posible, puesto que, según el reglamento, debemos darle una respuesta en un plazo de 10 días. Algunos ejemplos de ello son:
  - Un participante de un proyecto de investigación solicita la supresión de sus datos.
  - Una persona suscrita a nuestra *newsletter* solicita la baja.
  - Un/a estudiante manifiesta su deseo de no recibir más información sobre nuestra oferta formativa.

i) Formación específica en materia de protección de datos personales

- ISGlobal organiza sesiones específicas sobre protección de datos personales. Es importante asistir a dichas sesiones de formación para estar al día respecto de cómo abordar la protección en materia de datos personales.
- Si desea organizar una sesión formativa *ad hoc* en materia de datos personales para su equipo, póngase en contacto con la DPD.

j) Delegada de protección de datos y grupo de trabajo en materia de protección de datos personales

- De conformidad con lo dispuesto en el RGPD, ISGlobal debe nombrar a un delegado de protección de datos personales (DPD). La DPD actual y la fecha de su nombramiento se indican en el siguiente Anexo. Póngase en contacto con su DPD si tiene cualquier duda sobre esta cuestión.
- ISGlobal dispone asimismo de un grupo de trabajo en el ámbito de la protección de datos personales. Los componentes actuales del grupo de trabajo se indican en el siguiente Anexo.

Política de protección de datos personales	Fecha de aprobación 05 Mayo 2021	Autor/a Delegada de protección de datos	Revisado por Miembros del grupo de trabajo en protección de datos (WG LOPD), M. Benet (estadístico), M. Guxens (Assistant RP) Comisión de Equidad y Género Coordinadora de Calidad	Aprobado por Comité de Dirección

5. DOCUMENTOS INTERNOS RELACIONADOS

Normativa de ISGlobal sobre el uso de recursos y servicios informáticos
Modelo de código deontológico (proyectos de la UE y apartado sobre ética aplicable a protocolos)

6. REFERENCIAS

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679)

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
(https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673)

Directrices Éticas y Protección de Datos. Comisión Europea
(http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf)

Ley 14/2007, de 3 de julio, de Investigación Biomédica (BOE núm. 159, 28826-28848)
(http://www.boe.es/boe/dias/2007/07/04/pdfs/A28826-28848.pdf)

Código de Buenas Prácticas Científicas del Parque de Investigación Biomédica de Barcelona (PRBB) y Adenda
(https://www.isglobal.org/documents/10179/2484371/Code+of+Good+Scientific+Practice/03ee46c2-b5e9-4658-9d16-0450f736f7ee)

7. HISTORIAL DE VERSIONES

Versión	Fecha	Aprobación / Revisión
01	14/03/2019	Primera versión aprobada por el Comité de Dirección Nota: La implementación de la política se llevará a cabo a lo largo del año 2019 para garantizar la implantación de todas las medidas necesarias. Por la presente se acuerda vincular esta política a las Directrices de Gestión de Datos, que actualmente se encuentran en proceso de desarrollo.
02	2021 05 05	Título del documento actualizado de Buenas prácticas en materia de protección de datos personales a Política de protección de datos personales. Información sobre el nuevo contenedor de papel disponible en la 4.ª planta de Campus Clínic. Sección 8 – Anexo. Referencia a la Evaluación de impacto relativa a la protección de datos realizada en junio de 2019. Sección 9 – Anexo. Información sobre el nuevo sistema en línea para comunicar incidencias en materia de datos personales en la Intranet. Sección 10 – Actualizar la lista de miembros del grupo de trabajo Sección 11 - Anexo sobre teletrabajo y movilidad - incluye las medidas propuestas por la Agencia Española de Protección de Datos

Política de protección de datos personales	Fecha de aprobación 05 Mayo 2021	Autor/a Delegada de protección de datos	Revisado por Miembros del grupo de trabajo en protección de datos (WG LOPD), M. Benet (estadístico), M. Guxens (Assistant RP) Comisión de Equidad y Género Coordinadora de Calidad	Aprobado por Comité de Dirección

8. ANEXO. CLÁUSULA DE PROTECCIÓN DE DATOS / PRIVACIDAD EN FUNCIÓN DE LAS ACTIVIDADES DE TRATAMIENTO

Versiones en curso de los siguientes documentos:

ÁREA DE INVESTIGACIÓN

ISG-DP-FORM-VoluntariosWeb
ISG-DP-FORM-ConsentFormResearch_Cat_Es_En

RECURSOS HUMANOS

ISG-DP-FORM-PoliticaPrivacidadOfertasTrabajo
ISG-DP-FORM-Informació_Compromís_Treballador
ISG-DP-FORM-Compromís_Confidencialitat_Estudiants

EDUCACIÓN Y FORMACIÓN

ISG-DP-FORM-MatriculacioCursos

COMUNICACIÓN

ISG-DP-FORM-Children_Image_Release
ISG-DP-FORM-Menores_Cesion_Uso_Imagenes
ISG-DP-FORM-Adult_Image_Release
ISG-DP-FORM-Adultos_Cesion_Imagenes

COMPRAS

ISG-DP-FORM-ModelContracteEncarregatTractament
ISG-DP-FORM-ModelCompromísConfidencialitat

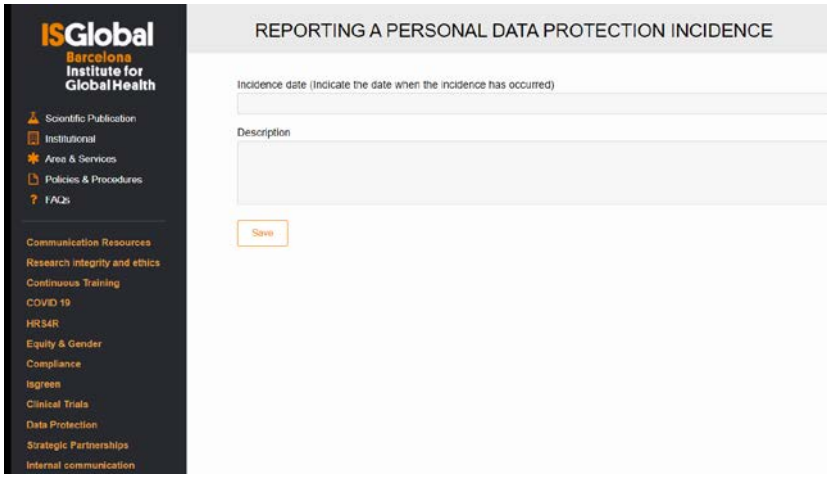
Política de protección de datos personales	Fecha de aprobación 05 Mayo 2021	Autor/a Delegada de protección de datos	Revisado por Miembros del grupo de trabajo en protección de datos (WG LOPD), M. Benet (estadístico), M. Guxens (Assistant RP) Comisión de Equidad y Género Coordinadora de Calidad	Aprobado por Comité de Dirección

9. ANEXO. EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS

La Evaluación de impacto relativa a la protección de datos institucional se llevó a cabo en junio de 2019 y cubre las áreas de Investigación y Comunicación. Los miembros del grupo de trabajo en materia de protección de datos realizan un seguimiento regular de las recomendaciones formuladas.

10. ANEXO. FORMULARIO DE COMUNICACIÓN DE INCIDENCIAS

Las incidencias en materia de protección de datos deben comunicarse utilizando el formulario en línea disponible en la Intranet. En caso de tener alguna pregunta o de que necesite ayuda con ello, puede ponerse en contacto con la DPD (lopd@isglobal.org).



Política de protección de datos personales	Fecha de aprobación 05 Mayo 2021	Autor/a Delegada de protección de datos	Revisado por Miembros del grupo de trabajo en protección de datos (WG LOPD), M. Benet (estadístico), M. Guxens (Assistant RP) Comisión de Equidad y Género Coordinadora de Calidad	Aprobado por Comité de Dirección

11. ANEXO. DPD Y GRUPO DE TRABAJO

Delegada de protección de datos: Joana Porcel (desde el 19 de diciembre de 2018)

Grupo de trabajo en materia de protección de datos

- Legal: Ramon Cifuentes y Ana Fort
- Informática: Paco Fernández
- Estadística: Sergi Sanz
- Investigación: Joana Porcel (delegada de protección de datos)
- RR. HH.: Samuel Espinal
- Comunicación: Aleix Cabrera
- Formación: Yolanda Amat
- Compras: Adrián Somoza

Política de protección de datos personales	Fecha de aprobación 05 Mayo 2021	Autor/a Delegada de protección de datos	Revisado por Miembros del grupo de trabajo en protección de datos (WG LOPD), M. Benet (estadístico), M. Guxens (Assistant RP) Comisión de Equidad y Género Coordinadora de Calidad	Aprobado por Comité de Dirección

12. ANEXO. RECOMENDACIONES ESPECÍFICAS PARA SITUACIONES DE TELETRABAJO Y MOVILIDAD

En abril de 2020, la Agencia Española de Protección de Datos emitió un conjunto de recomendaciones en materia de protección de datos para situaciones de teletrabajo y movilidad, como consecuencia en particular de la pandemia de la Covid19 (https://www.aepd.es/sites/default/files/2020-04/nota-tecnica-proteger-datos-teletrabajo.pdf).

La mayor parte de las recomendaciones se refieren a procedimientos generales que deben aplicarse al tratar datos personales y que poseen especial pertinencia para las situaciones de teletrabajo o movilidad. En este sentido, léanse con detenimiento las secciones 4b y 4c.

RECOMENDACIONES PERTINENTES QUE DEBEN SEGUIRSE: PROTECCIÓN Y COMUNICACIÓN

En situaciones de teletrabajo o movilidad existen algunas cuestiones específicas a las que hay que atender relacionadas con el hecho de trabajar en espacios públicos y con la necesidad de imprimir documentos:

- Para **trabajar en espacios públicos** (biblioteca, cafetería, aeropuerto) es necesario adoptar algunas medidas específicas:
    - NO DEJAR ningún dispositivo DESATENDIDO;
    - Estar atento/a a las PERSONAS QUE ESTÉN CERCA y proteger la información que pueda estar visualizando en pantalla;
    - Extremar las precauciones a la hora de entablar conversaciones; Encontrar un LUGAR EN EL QUE HAYA CIERTA INTIMIDAD y estar atento/a a las personas que estén cerca de usted.
- **Imprimir documentos**:
    - Se recomienda EVITAR IMPRIMIR DOCUMENTOS que contengan datos personales.
    - Si es de todo punto inevitable, deben seguirse las siguientes instrucciones:
        - NO DEJAR los documentos DESATENDIDOS, conservarlos bajo llave o archivarlos en un lugar privado;
        - Los documentos NO DEBEN SER DESECHADOS EN UN CUBO O CONTENEDOR PÚBLICO ni en la basura de casa.
        - Para destruirlos, puede o bien TRAERLOS a la oficina y echarlos al contenedor de papel o destruirlos en la DESTRUCTORA DE PAPEL, o bien romperlos en trozos pequeños que colocar en DIFERENTES CONTENEDORES.

- INFORMAR INMEDIATAMENTE. Si detecta o sospecha que la seguridad de los datos que está gestionando se ha visto comprometida, debe comunicar de forma inmediata una incidencia en materia de protección de datos (véase el Anexo 9).

Política de protección de datos personales	Fecha de aprobación 05 Mayo 2021	Autor/a Delegada de protección de datos	Revisado por Miembros del grupo de trabajo en protección de datos (WG LOPD), M. Benet (estadístico), M. Guxens (Assistant RP) Comisión de Equidad y Género Coordinadora de Calidad	Aprobado por Comité de Dirección

En situaciones de teletrabajo o movilidad, las medidas informáticas poseen especial pertinencia. Para una descripción pormenorizada, rogamos lea con detenimiento el **anexo específico sobre la política de recursos y servicios informáticos** (ISG-IT-POL-Normativa de ISGlobal sobre el uso de recursos y servicios informáticos). Estas son las medidas más pertinentes:

- Sus dispositivos (portátil, móvil) deben estar PROTEGIDOS CON UNA CONTRASEÑA SÓLIDA que difiera de las utilizadas para acceder a sus dispositivos personales o redes sociales

- NO utilice ni INSTALE otras APLICACIONES o programas en los equipos de empresa que utilice en situaciones de teletrabajo o movilidad a menos que hayan sido previamente autorizadas por SRI.

- El uso de EQUIPOS PERSONALES tan solo se permitirá en casos EXCEPCIONALES y debidamente justificados, siempre que el sistema operativo y el antivirus del equipo hayan sido debidamente actualizados. Si se ve obligado/a a utilizar un dispositivo personal, mantenga claramente separadas su información personal de la información profesional.

- El ACCESO REMOTO a los servicios de red y recursos internos (Intranet, SAPBO, Web-Purchasing, carpetas compartidas en red, servidores informáticos, etc.) se efectuará en todos los casos a través de una conexión remota segura VPN suministrada por la institución y gestionada por el equipo de SRI.

- La información que contenga datos personales o confidenciales debe CONSERVARSE en todo momento en el archivo de la RED INTERNA de ISGlobal o en el entorno GDrive institucional, con acceso remoto únicamente a través de VPN. Dicha información no debe descargarse en dispositivos locales (equipos personales o móviles) ni transferirse a personal no autorizado bajo ningún concepto, y su tratamiento debe ajustarse a la normativa vigente en materia de protección de datos (RGPD). NO se autoriza el uso de WhatsApp, Dropbox, Google Drive personal ni ninguna otra aplicación móvil no corporativa.

- No deben utilizarse conexiones wifi públicas o externas.

- Si recibe un correo electrónico sospechoso, no lo abra, en especial los documentos adjuntos que pueda incluir. Consulte primero al equipo de TI.

ARE YOU COMPLYING ON PRIVACY AND DATA PROTECTION?

Check the list below

Computer Access

It must be blocked (ctrl+alt+supr) when unattended. Power off when you leave work (the environment will also thank you).

Credentials Always Safe

Credentials are personal and non-transferable. Note that the password must be changed periodically, according to established procedure and IT regulations.

Data Storage

All files with personal data must be stored at the ISGlobal's internal server with restricted access, do not leave files with personal data in your desktop.

Do not keep files with personal data in removable storage devices (memory sticks, portable hard drives, and others) neither in your home computer.

Data Transportation

Personal data must not be stored or transported in removable storage devices (memory sticks, portable hard drives, and others) neither in home computers.

Personal Data

Any information relating to an identified or identifiable natural person.

Health, Biometric & Genetic Data

Special categories of personal data.

(We recommend you to apply the same criteria for confidential information.)

Data Sharing & Transfer

Do not transfer personal data to third parties without first consulting institutional procedures and current regulations. To share or transfer information, only secure tools provided by the SRI team are allowed. If necessary contact the DPO and the SRI team.

Printing

Avoid printing documents with personal data. If necessary do not leave documents untattended at the printer.

Secure Data Deletion

Empty the computer recycled bin after deleting any document containing personal data.

Documents containing personal data should be destroyed. Use the paper shredder or Confidential Document container.

Suspicious Mails

Beware of suspicious phishing emails, if in doubt do not open attachments and never provide your own credentials (username / password) to anyone. Contact the SRI team.

DATA INCIDENCES

Inform using the Intranet form (e.g. laptop / mobile stolen / lost; lost signed informed consents; receiving personal data through the email; contact by participants to exercise their rights).

Data breaches must be informed to the Spanish Agency within 72 hours

Breaches: accidental / unlawful destruction, loss, alteration, unauthorised disclosure or access.

QUESTIONS

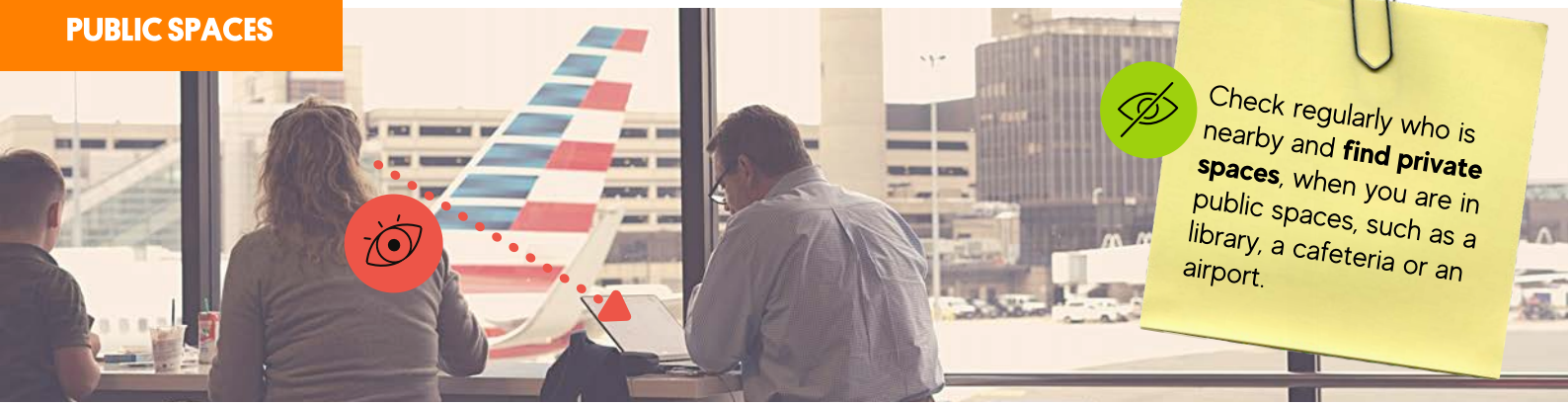
Read carefully the Personal Data Protection Policy available at the Intranet.

Contact the Data Protection Officer (DPO)
lopd@isglobal.org

ISGlobal

Processing Personal Data in Teleworking and Mobility Situations — Protect and Communicate

PUBLIC SPACES



Check regularly who is nearby and **find private spaces**, when you are in public spaces, such as a library, a cafeteria or an airport.

PRINTING DOCUMENTS

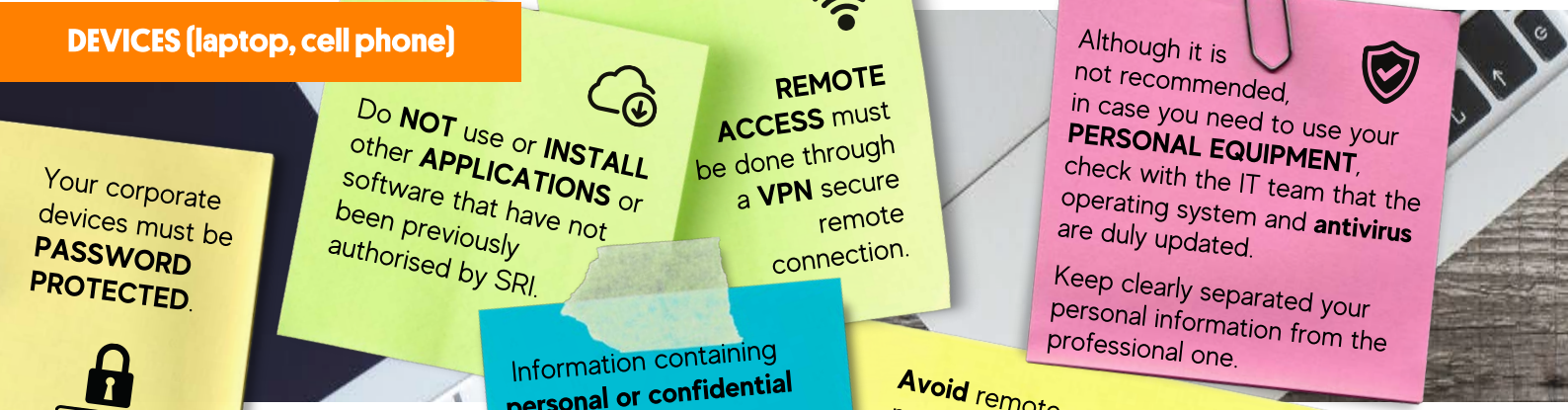
Avoid printing. If necessary...

Do **NOT** use **public bins** or household garbage for disposing the documents!

Bring them **BACK to the office**.

Or EXCEPTIONALLY dispose them in small pieces into **SEPARATE CONTAINERS**.

DEVICES (laptop, cell phone)



Your corporate devices must be **PASSWORD PROTECTED**.

Do **NOT** use or **INSTALL** other **APPLICATIONS** or software that have not been previously authorised by SRI.

REMOTE ACCESS must be done through a **VPN** secure remote connection.

Although it is not recommended, in case you need to use your **PERSONAL EQUIPMENT**, check with the IT team that the operating system and **antivirus** are duly updated.

Keep clearly separated your personal information from the professional one.

Information containing **personal or confidential data** must always be STORED in the **INTERNAL NETWORK** repository of ISGlobal or institutional GDrive environment, and with remote access only through VPN.

Avoid remote connection to the corporate network from public places, as well as connections via open, **unsecure WiFi** networks.

Communicate fast any incidence on personal data protection

If you detect or suspect that the data that you are managing has been compromised, immediately communicate a personal data incidence.
BREACHES MUST BE INFORMED TO THE SPANISH AGENCY WITHIN 72 HOURS.

Questions

Read carefully the Personal Data Protection Policy available at the Intranet.

Contact the DPO

lopd@isglobal.org

ISGlobal

ISGlobal

Normativa sobre Uso de Recursos y Servicios Informáticos

Barcelona, abril de 2022

Normativa sobre uso de recursos y servicios informáticos de ISGlobal	**Versión** 5	**Fecha de elab./rev.:** abril 2022	**Elaborado Por:** SRI/ Legal	**Aprobado por:** GM/DPO

NORMATIVA SOBRE USO DE RECURSOS Y SERVICIOS INFORMÁTICOS DE ISGLOBAL

(Dirigido al personal laboral y a personal colaborador externo)

A los efectos del presente documento se tendrán en consideración las siguientes definiciones:

- ***Institución***: la Fundación Privada Instituto de Salud Global Barcelona (ISGlobal)

- ***Redes de Comunicación***: la infraestructura de telecomunicaciones con acceso por parte de los Usuarios/as de la Institución, ya sea red interna o intranet, red externa o internet, correo electrónico (email), o cualquier otra herramienta de comunicación o transmisión telemática o de acceso a la información, mediante la conexión de equipos informáticos propiedad o gestionados por la Institución.
- ***Usuarios/as:*** toda persona física con acceso autorizado a los sistemas de información o redes de comunicación y con relación activa en el módulo de RRHH de la Intranet de la Institución.

- ***Recursos informáticos:*** todo aquel medio de naturaleza física, lógica o humana, que interaccione en los sistemas de información y redes de comunicación de la Institución.

- ***Aplicación informática:*** Programa o conjunto de programas informáticos necesarios para la gestión y tratamiento electrónico de la información.

Normativa sobre uso de recursos y servicios informáticos de ISGlobal	**Versión** 5	**Fecha de elab./rev.:** abril 2022	**Elaborado Por:** SRI/ Legal	**Aprobado por:** GM/DPO

SECCIÓN A): ÁMBITO DE APLICACIÓN DEL DOCUMENTO

El presente documento tiene carácter normativo y está dirigido a las personas usuarias que, para realizar sus funciones, requieren de un acceso continuado a las instalaciones de la Institución y a sus sistemas de información mediante el uso de sus recursos informáticos.

La finalidad del documento es facilitar a los Usuarios/as de la Institución la información relevante y las condiciones aplicables para el uso racional y optimizado de los Recursos Informáticos de la Institución.

ISGlobal cuenta actualmente con dos ubicaciones físicas distintas (instalaciones sitas en el Campus Clínic e instalaciones sitas en el Campus Mar) y éstas se encuentran dentro de instalaciones y espacios gestionados por una entidad tercera, por lo que determinadas cuestiones reguladas en el presente documento podrán ser tratadas de manera distinta en función de la ubicación en la que se encuentren los Usuarios/as en cuestión.

El presente documento debe ser entregado por el Departamento de RRHH a los Usuarios/as, una vez dados de alta en el sistema y con anterioridad a la incorporación a sus funciones profesionales y, en todo caso, previamente a su acceso a cualquiera de los sistemas informáticos u otros recursos de ISGlobal. Cuando la persona acceda por primera vez en la Intranet deberá aceptar la normativa actual.

Puede accederse a la última versión del presente documento en el módulo SRI de la Intranet: NORMATIVA_USO_RECURSOS_Y_SERVICIOS_INFORMÁTICOS

Toda actualización del documento será oportunamente comunicada a los Usuarios/as para su oportuno conocimiento.

A los efectos de acreditar la puesta a disposición de ISGlobal del siguiente documento, los Usuarios/as deberán firmar la Declaración Responsable que consta en el Anexo 3 posterior.

Normativa sobre uso de recursos y servicios informáticos de ISGlobal	Versión 5	Fecha de elab./rev.: abril 2022	Elaborado Por: SRI/ Legal	Aprobado por: GM/DPO

SECCIÓN B): NORMATIVA RELATIVA AL USO DE MEDIOS INFORMÁTICOS

Todo lo indicado en el presente apartado se ha especificado para la realización y consecución de un uso racional y optimizado de los Recursos Informáticos, así como también para el cumplimiento de lo dispuesto en el *Reglamento (UE) 2016/679 General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.*

Los Recursos Informáticos (incluida la infraestructura de comunicaciones) son gestionados por el Servicio de Recursos Informáticos de ISGlobal (en adelante, SRI), y en casos puntuales en colaboración con, el personal del departamento informático del Hospital Clínic de Barcelona (Campus Clínic) o el personal de los Servicios Informáticos del Parc de Recerca Biomèdica de Barcelona (Campus Mar)

Además de la presente normativa, se cumplirán las normas específicas establecidas por SRI. Cualquier solicitud, deficiencia, o mal funcionamiento de los Recursos Informáticos se comunicará a SRI mediante la generación de una incidencia informática en la Intranet dentro del módulo de SRI, o por email sri.tic@isglobal.org o en caso de urgencia comunicarlo por teléfono 932147373(ext. 7373) Campus Mar / 932174178 (ext.4178) Campus Clínic.
Se informará periódicamente sobre las características, prestaciones y novedades sobre los servicios y Recursos Informáticos existentes en ISGlobal.
Solo podrán utilizar los servicios y Recursos Informáticos de ISGlobal las personas vinculadas contractualmente con ISGlobal o personal colaborador externo, que hayan sido debidamente acreditadas por el Servicio de Recursos Humanos de ISGlobal y tengan relación activa en módulo RRHH de la Intranet.

B.1. SOBRE EL USO DE RECURSOS INFORMÁTICOS

B.1.1 Acceso a la Información (usuario/a informático y contraseña):

a) El Usuario/a con acceso al sistema de información dispondrá de una única autorización de acceso, personal e intransferible, compuesta al menos de identificador de usuario y una contraseña, que será de su conocimiento exclusivo.

b) Las credenciales (usuario/a y contraseña) se entregan al Usuario/a por primera vez en documento de papel por parte de RRHH (con contraseña de un solo uso) una vez formalizada su relación con la Institución. Cuando el Usuario/a accede por primera vez a su ordenador, debe cambiar la contraseña por una a su elección. La contraseña tendrá una longitud mínima de 8 caracteres. Los caracteres deben ser una mezcla de letras y números o caracteres especiales. Es obligado cambiar la contraseña cada 180 días y también es posible cambiarla de manera voluntaria a través de INTRANET setup.

Normativa sobre uso de recursos y servicios informáticos de ISGlobal	**Versión** 5	**Fecha de elab./rev.:** abril 2022	**Elaborado Por:** SRI/ Legal	**Aprobado por:** GM/DPO

c) Los Usuarios/as deben custodiar convenientemente su identificador de usuario/a y/o contraseña, sin proceder a su revelación o puesta al alcance de terceros. Serán responsables de toda la actividad relacionada con el uso de su acceso personal autorizado.

d) El Usuario/a recibirá notificaciones por email del sistema con avisos previos a la fecha de caducidad de la misma. De no haberse modificado antes de la fecha límite, la cuenta será bloqueada automáticamente y se deberá contactar con SRI para su desbloqueo y posterior cambio obligatorio.

e) Si los Usuarios/as sospechan que su acceso autorizado (identificador de usuario y/o contraseña) está siendo utilizado por otra persona, deberá proceder inmediatamente al cambio de contraseña y notificar la correspondiente incidencia.

f) Los Usuarios/as no deben intentar obtener otros derechos de acceso al suyo personal, ni utilizar ningún otro acceso autorizado que corresponda a otro Usuario, aunque disponga de la autorización de éste, salvo en los supuestos permitidos por la Ley o conforme a las instrucciones que imparta la Institución.

B.1.2 Adquisición y uso de equipos informáticos:

Respecto a la utilización de los equipos informáticos propiedad de ISGlobal cuyo uso tenga atribuido el Usuario/a , en general, se establece que:

a) Toda adquisición de equipos informáticos es propiedad de ISGlobal, debe ser homologada antes por SRI y realizada mediante el Servicio de Compras de la Institución, para garantizar una mayor integración y seguridad con los sistemas existentes.

b) El uso de los equipos informáticos facilitados por ISGlobal a su personal o personal colaborador es exclusivamente para el desarrollo de las funciones que tengan asignadas por parte de la Institución, sin que en ningún caso puedan ser utilizados para fines o actividades particulares.

c) Se hará un uso racional de los Recursos Informáticos y los Usuarios/as deberán cuidar los equipos informáticos facilitados, sin tratar de alterarlos o modificarlos. Solo personal SRI autorizado podrá realizar tareas de reparación, instalación o mantenimiento.

d) Como norma general, los únicos equipos informáticos que se pueden conectar a la red interna de ISGlobal serán los que hayan sido adquiridos por ISGlobal y hayan sido instalados y configurados por SRI Los equipos informáticos particulares sólo se pueden conectar a la red de invitados o Wi-fi, y sólo en casos excepcionales, previa supervisión de SRI, y tras ser adaptados a las directrices técnicas y seguridad de la infraestructura informática, se podrían conectar a la red interna.

Normativa sobre uso de recursos y servicios informáticos de ISGlobal	Versión 5	Fecha de elab./rev.: abril 2022	Elaborado Por: SRI/ Legal	Aprobado por: GM/DPO

e) Los equipos informáticos no se podrán extraer de las oficinas de ISGlobal a excepción de los ordenadores portátiles y los dispositivos de almacenamiento extraíbles, y en ningún caso se podrán hacer copias o extraer información que contenga datos de carácter personal y/o tenga carácter confidencial, sin una autorización previa y por escrito de la Gerencia de ISGlobal.

f) Si por motivos profesionales, fuera necesario utilizar el equipo informático asignado fuera de los espacios ISGlobal, se deberá firmar previamente el "*Acuerdo de cesión de uso de equipo informático*", donde se formaliza un acuerdo que permite la salida temporal de equipos informáticos.Para los supuestos de donación de equipos obsoletos, se deberá firmar en todo caso el modelo de " *Contrato de Donación de equipo informático*".

g) En caso de robo o extravío de equipos propiedad de ISGlobal se deben aplicar las siguientes acciones descritas en este protocolo "*Protocolo ante el robo o hurto de equipos propiedad de ISGlobal"*

B.1.3 Utilización de aplicaciones informáticas

En general se establece que:

a) En los equipos de ISGlobal sólo se pueden hacer instalaciones de aplicaciones legalmente utilizables, es decir, aplicaciones informáticas con la correspondiente licencia y compradas por ISGlobal o aplicaciones informáticas cuya licencia permita el uso gratuito y cuyo uso haya sido aprobado previamente por SRI. Las aplicaciones informáticas no adquiridas por ISGlobal deberán estar autorizadas por escrito por personal responsable de SRI.

b) Queda **prohibido expresamente** la instalación de aplicaciones informáticas sin la correspondiente licencia o que no se adecue a la legislación vigente. También queda prohibido expresamente instalar o utilizar aplicaciones informáticas con licencia propiedad de ISGlobal en equipos informáticos personales (no corporativos)

c) El equipo SRI será el responsable de configurar o reinstalar el sistema operativo del equipo informático, y dará soporte (instalación, mantenimiento, y desinstalación) a las aplicaciones informáticas verificadas y aprobadas por SRI, que cumplan con las condiciones de uso establecidas, y destinadas a las funciones profesionales inicialmente designadas.

d) Los Usuarios/as no pueden hacer copias de las aplicaciones informáticas excepto en los casos autorizados por SRI, ni desinstalar las aplicaciones informáticas proporcionadas por la Institución. Se limitarán a ejecutar las aplicaciones informáticas legalmente instaladas y para las que estén autorizados.

Normativa sobre uso de recursos y servicios informáticos de ISGlobal	**Versión** 5	**Fecha de elab./rev.:** abril 2022	**Elaborado Por:** SRI/ Legal	**Aprobado por:** GM/DPO

e) Los Usuarios/as están obligados a cumplir las medidas de seguridad previstas por la Institución, así como las prevenciones que al efecto se establezcan. Por lo tanto, no se podrán desactivar los programas antivirus ni sus actualizaciones, y tampoco podrán introducir de manera voluntaria programas, virus o malwares que puedan causar alteración o daños en el sistema y afectar la seguridad de la red.
Si un programa puede afectar a la seguridad y/o vulnerabilidad del resto de la infraestructura informática o alterar su correcto funcionamiento, podrá ser retirado por SRI.

f) Queda prohibida cualquier actuación que pueda tener consideración de provocadora o intimidatoria en el trabajo, de tal manera, que debe excluirse la instalación o visualización de salvapantallas, fotos, vídeos, comunicaciones u otros medios con contenidos ofensivos, violentos, amenazadores, obscenos o, en general, aquellos que agredan la dignidad de la persona.

B.1.4. Medidas de Seguridad en los Medios Informáticos:

a) Equipos portátiles y dispositivos extraíbles (discos externos, pendrives, etc..): deberán quedar guardados bajo llave o protegidos bajo contraseña cuando el Usuario/a no se encuentre presente.
Los Usuarios/as pueden utilizar dispositivos de almacenamiento externo para intercambiar documentos y datos con otros sistemas informáticos siempre que no se trate de datos confidenciales y/o de carácter personal. Si se detecta que un Usuario/a está haciendo un mal uso de los mismos (por peligro de propagación de virus u otras causas) se le retirará esta posibilidad hasta que SRI tenga la certeza de que ya no representa una amenaza para el resto de usuarios ni para los sistemas informáticos.

b) Para todos los equipos informáticos: se cerrará o bloquearán bajo contraseña, todas las sesiones en el supuesto de ausentarse temporalmente de su puesto de trabajo, a fin de evitar accesos no autorizados (uso del protector de pantalla con sesión bloqueada mediante contraseña). Al término de la jornada, se apagarán los dispositivos informáticos (ordenadores, portátiles, etc.) incluidas las pantallas, a excepción de aquellos ordenadores que estén realizando una tarea que requiera que se mantengan encendidos (en este caso se notificará a SRI).

c) Inspección y control de medios informáticos y acceso por parte de ISGlobal: ISGlobal podrá introducir filtros de control, bloqueo y/o borrado de correos y páginas web que considere no necesarios para la realización de las tareas asignadas en todos los medios informáticos de su propiedad. El Usuario/a deberá abstenerse de intentar modificar los medios informáticos en cualquier sentido. Los medios informáticos podrán ser objeto de inspección por parte de ISGlobal o persona en la que se delegue a tal efecto, sin que en ningún caso deba considerarse intromisión en la intimidad del Usuario/a.
Se considera razonable el acceso y control a los medios informáticos dispuestos por parte de ISGlobal cuando sea necesario:

Normativa sobre uso de recursos y servicios informáticos de ISGlobal	Versión 5	Fecha de elab./rev.: abril 2022	Elaborado Por: SRI/ Legal	Aprobado por: GM/DPO

- Para vigilar el cumplimiento por parte del Usuario/a de sus obligaciones (incluyendo el uso que se hace de los medios informáticos) en casos específicos que así lo requieran.

- Para coordinar y garantizar la continuidad de las tareas asignadas en los supuestos de ausencias de los Usuarios/as.

- Para proteger la red de comunicaciones y el sistema informático de la Institución.

- Para prevenir responsabilidades de la Institución que pudieran derivarse también algunas formas ilegales o ilícitas de uso frente a terceros.

B.1.5 Uso de la información gestionada en los sistemas

a) Toda la información albergada en los servidores de ISGlobal , o que circule a través de su red mediante elementos de comunicación o transmisión, que sean de su propiedad o le hayan sido confiada, tiene carácter confidencial.

b) Los Usuarios/as con acceso a información y datos deben usarlos únicamente para las operaciones para las que fueron generados e incorporados, sin destinarlos a otros fines o incurrir en actividades que puedan considerarse ilícitas o ilegales. Asimismo, sólo deben acceder a aquellos datos y recursos que precisen para el ejercicio de las funciones que les correspondan, y efectuar sólo los tratamientos que sean precisos para el cumplimiento de los fines de la Institución.

c) Los Usuarios/as están obligados a proteger la información, evitando el envío no autorizado al exterior, incluyendo esta noción tanto el acceso como la visualización de la misma. Una especial consideración de confidencialidad corresponde a ficheros o información que contenga datos de carácter personal, ya que su tratamiento inadecuado puede ser constitutivo de infracciones que podrían conllevar sanciones de cuantía elevada a esta Institución.

d) Los Usuarios/as, conforme a las instrucciones que reciban, utilizarán los medios o programas de salvaguarda que les facilite la Institución, con la finalidad de garantizar la integridad y seguridad de los equipos informáticos, de las aplicaciones informáticas y de la información que contengan. En cualquier caso, no intentarán descifrar claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervengan en los procesos telemáticos

e) Los Usuarios/as están obligados a notificar cualquier incidencia o anomalía en el uso de los medios informáticos que puedan detectar: pérdida de información, de listados o de disquetes, acceso no autorizado, uso de su identificador de

Normativa sobre uso de recursos y servicios informáticos de ISGlobal	**Versión** 5	**Fecha de elab./rev.:** abril 2022	**Elaborado Por:** SRI/ Legal	**Aprobado por:** GM/DPO

usuario o de su contraseña, introducción de virus, recuperación de datos, desaparición de soportes informáticos y, en general, toda situación que pueda comprometer el buen uso y funcionamiento de los sistemas de información.

f) Los Usuarios/as autorizados a manejar soportes que contengan datos de carácter personal deben guardarlos en lugar seguro, especialmente al finalizar la jornada laboral. En todo caso, una vez concluida la finalidad de las tareas a las que estaban destinados estarán obligados a su devolución inmediata.

g) Si un Usuario/a finaliza su relación con la Institución o se traslada de puesto de trabajo, deberá dejar sin perjudicar todas las aplicaciones informáticas, ficheros, información, datos y documentos electrónicos que haya utilizado en su actividad profesional. Una vez finalizada la relación con la Institución, dejará de tener acceso a los equipos informáticos y a la información incorporada a los mismos, debiendo devolver aquellos que se encuentren en su posesión. Seguirá obligado a mantener la máxima reserva y confidencialidad, no sólo de la información y documentos, sino también de las claves, análisis y aplicaciones informáticas que haya conocido durante o con motivo de su relación con la Fundación.

B.1.6 Información Web Corporativa y Web de Proyectos

a) toda la información publicada en la web corporativa es de titularidad de ISGlobal y debe de ser autorizada previamente por el personal responsable designado por el Departamento de Comunicación.

b) la implementación de una nueva web de proyecto debe de ser notificada antes a Departamento de Comunicación y SRI para su previa evaluación técnica, mediante solicitud vía formulario web
No se podrá registrar ni dar de alta ningún dominio web titularidad de ISGlobal sin que éste cumpla con los requisitos exigidos por la normativa sobre protección de datos (Reglamento UE 2016/679 y Ley 3/2018) y sobre servicios de la sociedad de la información y comercio electrónico (Ley 34/2002). A tales efectos, todo dominio web deberá disponer del preceptivo aviso legal y de una política de privacidad y uso de cookies validada por la Delegada de Protección de Datos de ISGlobal (lopd@isglobal.org).

c) el trabajador/a tiene la opción de modificar la configuración de derechos de imagen para uso institucional, mediante el apartado Configuración de Privacidad de la Intranet.

B.1.7. Almacenamiento y copias de seguridad de ficheros informáticos:

a) Como norma general, todos los datos de titularidad ISGlobal, se deben guardar en el servidor institucional, dentro de una carpeta de la red interna

Normativa sobre uso de recursos y servicios informáticos de ISGlobal	**Versión** 5	**Fecha de elab./rev.:** abril 2022	**Elaborado Por:** SRI/ Legal	**Aprobado por:** GM/DPO

debidamente protegida por SRI, para garantizar la integridad y seguridad de la información.

b) No está autorizado el uso de servicios externos personales de almacenamiento como "cloud storage" (Dropbox, Google Drive particular, etc.), así como dispositivos de almacenamiento externo (pendrives, HD externos, etc..) para datos de carácter personal y/o confidencial, que pudieran facilitar la copia o transferencia no autorizada de los datos.

c) En aquellos casos en que sea posible se evitará la ubicación de ficheros que contengan datos de carácter personal en los equipos de Usuarios/as. Los Usuarios/as sólo podrán crear ficheros temporales que contengan datos de carácter personal cuando sean necesarios para el desempeño de sus funciones, en todo caso, deberán ser eliminados cuando hayan dejado de ser útiles para la finalidad para la que fueron creados.

d) De las copias de seguridad de los datos almacenados en los discos locales se responsabilizará el propio Usuario/a, y no deberán contener información de carácter personal y/o confidencial.

e) El equipo SRI, mediante un plan global de mantenimiento, realiza copias de seguridad diarias de los archivos e información almacenados en los servidores corporativos en un repositorio independiente destinado a backup y de acceso restringido al personal SRI.

B.1.8. Envío de Información:

a) Los Usuarios/as tienen prohibido el envío de categorías sensibles de datos, salvo autorización expresa de la Delegada de Protección de Datos o persona que tenga asignada esta función. En todo caso, este envío únicamente se podrá realizar si se adoptan los mecanismos necesarios para evitar que la información sea inteligible y/o manipulada por terceros, tales como protocolos de transferencia segura de datos proporcionada por SRI.

b) Para el envío de información de carácter personal, nunca debe de realizarse a través de redes públicas o redes inalámbricas externas (incluyendo el envío por correo electrónico), y es obligatorio al cifrado de datos o la utilización de cualquier otro mecanismo de encriptación que garantice que la información no sea inteligible ni manipulada por terceros.

c) Así se establece, que se podrá enviar mediante correo electrónico encriptado siguiendo lo establecido en el apartado (b) anterior.

d) Sin embargo, como norma general, se recomienda no hacer envío de datos de carácter personal, para lo cual sería necesario enviar los datos anonimizados (disociados) para evitar la identificación de los mismos con el sujeto fuente.

Normativa sobre uso de recursos y servicios informáticos de ISGlobal	**Versión** 5	**Fecha de elab./rev.:** abril 2022	**Elaborado Por:** SRI/ Legal	**Aprobado por:** GM/DPO

e) El uso de certificados digitales: Se recomienda, para garantizar la validez y eficacia de la emisión y recepción de comunicaciones y documentos producidos telemáticamente, el uso de la firma electrónica.

B.1.9 Acceso a las redes de comunicación:

SRI gestiona la conexión de los Usuarios/as y sus equipos corporativos a las redes de comunicación (red interna e internet). Asimismo, SRI gestiona y monitoriza el tráfico de red existente, implementando los filtros y reglas de seguridad a nivel de Firewall, para garantizar la seguridad e integridad de la red y los recursos internos de la Institución.

Queda expresamente prohibido:

a) Conectarse a la red interna de comunicaciones por otros medios distintos a los definidos y administrados por la Institución.

b) Acceder al sistema informático utilizando identificadores y contraseñas de otros Usuarios/as (suplantación de identidad)

c) Evitar las medidas de seguridad establecidas en el sistema informático, intentando acceder a ficheros o aplicaciones informáticas cuyo acceso no le haya sido permitido. Asimismo, no deben intentar distorsionar o falsear los registros logs de los sistemas de información.

d) El empleo de la red corporativa (sistemas informáticos y cualquier medio puesto al alcance del Usuario/a) vulnerando el derecho de terceros, los propios de la organización, o bien para la realización de actos que pudieran ser considerado ilícitos.

e) Instalar, salvo autorización expresa del Delegado de Protección de Datos o el personal que tenga asignada esta tarea (SRI), cualquier tipo de aplicación informática o dispositivo ni en los servidores centrales ni en el ordenador empleado.

B.1.10. Conexiones para invitados y visitantes:

Existe una conexión con acceso a internet por wifi, (“prbb” en Campus Mar, “isglobal” en Campus Clínic) para visitantes o estancias temporales. Debe consultarse a SRI las condiciones y las credenciales para establecer la conexión.

Adicionalmente, existe un servicio de conexión cableada con acceso a Internet mediante una red aislada (“Convidats” a Campus Mar) para portátiles personales y otros dispositivos externos, que no dispongan de cobertura Wi-Fi adecuada o no

Normativa sobre uso de recursos y servicios informáticos de ISGlobal	**Versión** 5	**Fecha de elab./rev.:** abril 2022	**Elaborado Por:** SRI/ Legal	**Aprobado por:** GM/DPO

cumplan con los requerimientos de seguridad de la red interna. Los criterios de conexión a esta red se deben de acordar, en cada caso, con el personal de SRI. Está conexión está específicamente diseñada para personas visitantes durante estancias temporales superiores a un mes y de carácter periódico.

B.2. SOBRE EL USO Y EL ACCESO A INTERNET

B.2.1. Acceso a internet:

a) El acceso a internet por los Usuarios/as se realizará únicamente empleando los medios y a través de la red establecida a estos efectos por la Institución.

b) La Institución podrá controlar los accesos a internet. En este sentido, se podrá proceder a monitorizar las direcciones de acceso y el tiempo de conexión de los usuarios a internet, así como la limitación de su uso en razón de las funciones que ejerza, por motivos de seguridad o rendimiento de la red.

B.2.2. La definición de la política de seguridad sobre uso de recursos informáticos de la Institución incluye las siguientes **prohibiciones** en referencia al uso de Internet:

a) Utilizar la red Internet, para actividades no directamente relacionadas con las tareas asignadas. Cualquier acceso a página web, intranet o enlace instalado o facilitado por ISGlobal se entenderá que lo es a efectos meramente profesionales.

b) Acceder a direcciones de internet que tengan un contenido ofensivo o atentatorio de la dignidad humana. A estos efectos, la Institución podrá restringir el acceso a determinados servidores de contenidos en internet.

c) Descargar software o archivos de cualquier tipo desde Internet, que no sean requeridos para el desempeño de la actividad profesional o sin consentimiento expreso de la entidad.

d) Introducir contenidos en la red corporativa y/o ordenador personal que no tengan relación con la actividad y objetivos de la Institución.

e) Infringir derechos de propiedad intelectual o de marcas respecto a materiales multimedia.

f) Obtener o almacenar información con contenidos que infrinjan las leyes o derechos de terceros.

g) Utilizar navegadores o aplicaciones informáticas fuera del estándar.

Normativa sobre uso de recursos y servicios informáticos de ISGlobal	**Versión** 5	**Fecha de elab./rev.:** abril 2022	**Elaborado Por:** SRI/ Legal	**Aprobado por:** GM/DPO

h) la instalación de sistemas proxy por los Usuarios/as.

i) utilizar la red para participar en chats para uso personal o juegos en línea.

j) Descargar o transmitir imágenes, sonido o vídeo que produzcan una saturación de la red.

B. 3. SOBRE EL USO DEL CORREO ELECTRÓNICO

B.3.1. Uso profesional: ISGlobal facilitará a todo su personal (con relación activa en el módulo RRHH de la Intranet) una cuenta de e-mail (Gmail) para uso estrictamente profesional, siéndole aplicable, en todo caso, lo señalado en el punto anterior, independientemente de que se acceda desde un equipo facilitado por ISGlobal o desde otro dispositivo externo cualquiera.

Una vez finalizada la relación laboral con ISGlobal se aplicará el procedimiento de baja de email descrito en el documento ISG-SRI-PROC Procedimiento e Instrucciones de baja de cuenta e-mail

B.3.2: La definición de la política de uso y control del correo electrónico incluye las siguientes **prohibiciones**:

a) Utilizar el correo electrónico para el envío de información que contenga categorías sensibles de datos personales, a menos que cuenten con autorización expresa del Delegado de Protección de Datos de ISGlobal. En todo caso, el envío de esta información se realizará siempre cifrando el correo (ver apartado B.1.8 Envío de Información), o bien adoptando cualquier otro tipo de protocolo (sFTP, PrivateCloud, etc.) que evite el acceso o manipulación de la información por terceros.

b) Enviar comunicaciones profesionales desde cuentas personales.

c) Leer, borrar, copiar o modificar mensajes o archivos dirigidos a otros Usuarios/as.

d) Utilizar identificadores y contraseñas de otros Usuarios/as para acceder al sistema email.

e) Revelar las direcciones de correo electrónico de otros destinatarios al reenviar mensajes

f) Enviar correos masivos, utilizando la dirección de correo electrónico corporativa de ISGlobal. En caso de ser necesario el envío de correos masivos, es necesario ponerse en contacto con SRI para evitar posibles problemas de filtrado de spam.

Normativa sobre uso de recursos y servicios informáticos de ISGlobal	**Versión** 5	**Fecha de elab./rev.:** abril 2022	**Elaborado Por:** SRI/ Legal	**Aprobado por:** GM/DPO

g) Extraer del servidor de Gmail de ISGlobal cualquier copia seguridad de la documentación que un empleado/a saliente haya generado o recibido en su buzón de correo electrónico corporativo durante su relación laboral. Tampoco está permitido reenviarse emails desde su cuenta Gmail institucional a su email personal

B.3.3. Smartphone o dispositivos móviles: en caso de necesitar configurar el correo electrónico de ISGlobal utilizando un smartphone o dispositivo móvil, éste deberá haber sido adquirido o comprado por ISGlobal y configurado y verificado por el personal de SRI. En ningún caso se utilizarán dispositivos personales para gestionar el e-mail que implique descarga de contenidos en la memoria del dispositivo, por ello se recomienda utilizar el webmail mediante la versión "mobile" de navegador web del dispositivo.

En caso de pérdida, robo, etc. del dispositivo se deberá notificar lo antes posible (máx. 24 h) al personal responsable de seguridad o al personal designado en ausencia de estos primeros. Una vez notificado, se procederá con el protocolo de seguridad, se realizará el registro de la incidencia y se bloqueará la sincronización del email con el dispositivo.

B.4. DEL PERSONAL (SRI) CON RESPONSABILIDADES EN LOS SISTEMAS DE INFORMACIÓN.

Se encontrarán exceptuados de aplicar las instrucciones precedentes que interfieran en su cometido aquellas personas adscritas a puestos de trabajo que tienen funciones de diseño, desarrollo, operación o administración de los sistemas de información y de las redes de comunicación (equipo SRI).

Sólo se entenderán autorizados para el ejercicio de tales funciones cuando sigan estrictamente las directrices de los responsables de la Institución. Además, deberán tener especial consideración con:

a) No acceder a la información o datos aprovechando sus privilegios de administración, excepto por motivos de seguridad o integridad del sistema, o cuando la persona responsable de la información o datos lo autorice expresamente.

b) Custodiar con especial cuidado los identificadores y contraseñas que den acceso a los sistemas con privilegio de administrador.

c) Procurar que la información almacenada y tratada por los sistemas de información sea salvaguardada mediante copias de seguridad y para la recuperación de datos periódicamente, al menos con carácter semanal, salvo que en dicho período no se haya producido actualización de los datos.

Normativa sobre uso de recursos y servicios informáticos de ISGlobal	**Versión** 5	**Fecha de elab./rev.:** abril 2022	**Elaborado Por:** SRI/ Legal	**Aprobado por:** GM/DPO

d) Que los soportes informáticos que contengan datos de carácter personal estén convenientemente registrados en un inventario actualizado, donde figure el tipo de información que contienen y las personas autorizadas a su manejo. Que se cumpla escrupulosamente el control de acceso restringido a personal autorizado en los locales, edificios o recintos en que se encuentren los sistemas de almacenamiento y servidores con información confidencial o con datos de carácter personal.

e) Notificar cualquier violación de las normas de seguridad o de vulnerabilidad de los sistemas de información que detecten, no revelando en ningún caso a terceros estas debilidades, excepto a la persona autorizada que reciba en el encargo de realizar los trabajos para su corrección.

SECCIÓN C): MEDIDAS DE SEGURIDAD Y RECOMENDACIONES PARA SITUACIONES DE MOVILIDAD Y TELETRABAJO

Las siguientes medidas de seguridad son aplicables en aquellas situaciones y/o escenarios (p.e. teletrabajo, desplazamientos al exterior, estancias temporales, etc.) y que por necesidades del proyecto o del personal empleado requiera acceder externamente, desde cualquier ubicación fuera de las oficinas de la institución, a los servicios y recursos de red internos de la institución.

Con el objetivo de reducir todo lo posible el riesgo de seguridad asociado a este tipo de conexiones externas, y evitar capturas de credenciales personales o de información sensible por parte de terceros, es obligatorio realizar estas conexiones remotas mediante un acceso debidamente protegido y con transmisión de datos cifrada, para poder garantizar la seguridad e integridad de los sistemas de información (SI) de ISGlobal.

A continuación, se describen las diferentes medidas de seguridad y recomendaciones específicas para proteger la información gestionada en situaciones de movilidad o teletrabajo:

a) El acceso remoto a los servicios y recursos de red interna (Intranet, SAPBO, Web-Compras, Carpetas compartidas de red, Computing Servers,..) se realizará en cualquier caso mediante conexión remota segura VPN proporcionada por la institución y gestionada por equipo SRI.

b) La conexión remota de cada empleado estará definida mediante un perfil y nivel de acceso específico, asociado a su categoría funcional y/o responsabilidades dentro del proyecto o área de gestión de la institución (Administración, Investigación, Formación, Comunicación, etc.)

Normativa sobre uso de recursos y servicios informáticos de ISGlobal	**Versión** 5	**Fecha de elab./rev.:** abril 2022	**Elaborado Por:** SRI/ Legal	**Aprobado por:** GM/DPO

c) Cada empleado obtendrá unas credenciales iniciales temporales de conexión (usuario/contraseña) de carácter personal e intransferibles, y deberá definir y utilizar una nueva contraseña robusta y diferente a las utilizadas para acceder a cuentas de correo personales, redes sociales y otro tipo de aplicaciones utilizadas en el ámbito personal. Estas credenciales deben renovarse cada 180 días.

d) Si el empleado detectara que su acceso personalizado (credenciales de usuario y/o contraseña) está siendo utilizado por otra persona, deberá notificarlo inmediatamente a SRI por los canales habituales de comunicación establecidos (teléfono o email), y proceder al cambio de su contraseña lo antes posible.

e) La información que contenga datos de carácter personal o confidencial, debe de almacenarse siempre en los repositorios de la red interna de ISGlobal o entorno GDrive institucional, y con acceso remoto solo mediante VPN. Esta información no debe ser descargada en dispositivos locales (equipo personal o móviles), ni transferida a personal no autorizado bajo ningún concepto, y su tratamiento debe ajustarse al reglamento vigente de protección de datos (RGPD).

f) Toda conexión remota mediante VPN debe realizarse con equipos o dispositivos institucionales, debidamente configurados y actualizados (sistema operativo, antivirus, etc.) evitando el uso de equipos personales o no corporativos, que estén fuera del control y gestión por parte de SRI.

g) Solo en casos excepcionales y debidamente justificados se permitirá el uso de equipos personales, y con el sistema operativo y el antivirus del equipo debidamente actualizados. Además, se debe evitar simultanear la actividad personal con la profesional, siendo necesario definir perfiles independientes para desarrollar cada tipo de tarea.

h) El acceso a las aplicaciones institucionales de Google Suite (Gmail, GDrive...) también puede realizarse mediante equipos personales, no corporativos o dispositivos móviles, sin embargo, debe extremarse la precaución de su uso, cumpliendo en todo momento con las medidas de seguridad establecidas por los sistemas de Google, con el objetivo de reducir riesgos y posibles brechas de seguridad.

i) Se debe tener especial atención cuando sea necesario utilizar dispositivos de uso público, en hoteles, workcenters, bibliotecas etc. evitando la descarga de información sensible y asegurarse de cerrar debidamente la sesión de usuario con el fin de evitar suplantaciones de identidad o posibles brechas de seguridad.

j) Se recomienda evitar todo lo posible, la conexión remota de los dispositivos a la red corporativa desde lugares públicos, así como la conexión mediante redes WIFI abiertas no seguras

k) Siempre debe verificarse la autenticidad y legitimidad de los correos electrónicos recibidos, comprobando que el dominio electrónico del remitente

Normativa sobre uso de recursos y servicios informáticos de ISGlobal	Versión 5	Fecha de elab./rev.: abril 2022	Elaborado Por: SRI/ Legal	Aprobado por: GM/DPO

es válido y conocido, y evitando la descarga de ficheros adjuntos con extensiones inusuales o el establecimiento de conexiones a través de enlaces sospechosos incluidos en el cuerpo del correo.

l) En los equipos corporativos utilizados para teletrabajo o en situaciones de movilidad, no está permitido utilizar ni instalar otras aplicaciones o software que no hayan sido previamente autorizados por SRI, y no deben ser utilizados con fines particulares o personales, evitando el acceso a redes sociales, correo electrónico personal, páginas web con reclamos y publicidad, así como otros sitios susceptibles de contener virus o favorecer la ejecución de código malicioso.

m) Se recomienda revisar y eliminar periódicamente la información residual que pueda quedar almacenada localmente en el dispositivo, como archivos temporales del navegador o descargas de documentos.

n) Una vez concluida la jornada de trabajo en situación de movilidad o teletrabajo, debe desconectarse la sesión de acceso remoto (VPN) y apagar o bloquear el acceso al dispositivo.

HISTORIAL DE VERSIONES

Versión	Fecha	Cambios	Aprobado por
1	Jan. 2019	Initial release	Direction Committee on 14th March 2019
2	Feb. 2020	Update section B1.3 (b) and Annex 1	LOPD Working Group
3	Oct. 2020	Update section B1.2 (g) and Annex 1-2	General Manager and DPO
4	May 2021	Section C added	General Manager and DP Group
5	Abr 2022	Se añade el punto 3.2 g	General Manager and DP Group

Guías funcionales relacionadas:

How to access remotely to ISGlobal network with VPN client

How to remotely change the ISGlobal network user password

Normativa sobre uso de recursos y servicios informáticos de ISGlobal	**Versión** 5	**Fecha de elab./rev.:** abril 2022	**Elaborado Por:** SRI/ Legal	**Aprobado por:** GM/DPO

ANEXO 1: Identificador de Perfiles – Personas

- **SRI**: Alberto Torres, Joan Vericat, Victor Boluda, Rubén Vidal, Manel Rodríguez, Marcos Rodríguez, José Luis Rodríguez, Shajal Shaikh, Paco Fernández
- **HR:** Samuel Espinal, Francesc Guil, Marta Guerrero, Maria José Merino, Alex Boix
- **LEGAL:** Ramón Cifuentes
- **PURCHASING:** Adrián Somoza, Francisco Tauste
- **GENERAL SERVICES:** Gemma Perelló, Fernando Andrés
- **COMMUNICATIONS:** Pau Rubio, Aleix Cabrera
- **RESEARCH MANAGEMENT & DPO**: Joana Porcel
- **GENERAL MANAGER:** Gonzalo Vicente

ANEXO 2: Documentación Relacionada

- Política de protección de datos personales
- Procedimiento de alta/renovación de dominios y websites
- Acuerdo de cesión de uso de equipo informático
- Modelo contrato de donación de equipo informático
- ISG-SRI-PROC- Procedimiento e Instrucciones de baja de cuenta e-mail
- ISG-SRI-POL-IT support for ISGlobal users: services and funding
- Protocolo ante el robo o hurto de equipos propiedad de ISGlobal

Normativa sobre uso de recursos y servicios informáticos de ISGlobal	**Versión** 5	**Fecha de elab./rev.:** abril 2022	**Elaborado Por:** SRI/ Legal	**Aprobado por:** GM/DPO

ANEXO 3: Declaración Responsable

DECLARACIÓN RESPONSABLE RELATIVA AL USO DE RECURSOS Y SERVICIOS INFORMÁTICOS DE ISGLOBAL

D./Dña [.], mayor de edad, provisto/a de DNI, NIE o Pasaporte número [.], por la presente declaro haber sido informado/a de los requisitos y condiciones a los que se sujeta el uso de recursos y servicios informáticos en la Fundación Privada Instituto de Salud Global Barcelona (ISGlobal), incluidas las obligaciones en materia de confidencialidad y protección de datos personales inherentes al uso de dichos recursos y servicios.

Las anteriores cuestiones se hallan reguladas en el documento denominado: "*Normativa sobre el uso de recursos y servicios informáticos en ISGlobal*", habiéndome sido facilitada una copia del mismo con carácter previo al ejercicio de mis funciones y al acceso a los recursos y sistemas informáticos de la entidad.

Asimismo, he sido debidamente informado/a por el Departamento de RR.HH de ISGlobal de que el incumplimiento de las obligaciones establecidas en el citado documento podrá ser considerado como una falta grave, imponiéndose las sanciones previstas para este tipo de faltas en la normativa laboral.

Todo lo cual declaro bajo mi responsabilidad, en Barcelona, a [.] de [.] de 20[.].

Nombre y Firma

PROTECCIÓN DE DATOS PERSONALES

ISGlobal
Barcelona
Institute for
Global Health

Institució
CERCA
Centres de Recerca
de Catalunya

Regulación

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

- **Agencia Española de Protección de Datos**
  https://www.aepd.es/index.html
- **Autoritat Catalana de Protecció de Dades**
  http://apdcat.gencat.cat/ca/inici/
- **European Data Protection Board**
  https://edpb.europa.eu/

Datos personales & categorías especiales de datos

toda información sobre una persona física **identificada** o **identificable** («el interesado»)

Categorías especiales de datos ("datos sensibles")

Origen étnico / racial, opiniones políticas, creencias religiosas o filosófocas, información sindical, datos **genéticos, biométricos** (con el propósito de identificar una personal natural), o datos de **salud**, datos sobre la vida u orientación sexual de una persona natural.

IDENTIFICADORES

Nombre
ID número
Localización / Geolocalización / Geotracking
Factores (físicos, fisiológicos, genéticos, mentales, económicos, culturales, de identidad social)
Combinación (enfermedades raras, sexo, fecha de nacimiento)
Voz / Imágenes

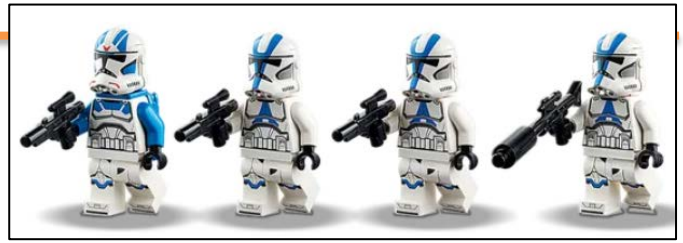
ISGlobal

Reglamento General de Protección de Datos (RGPD) – Privacidad por:

POR DISEÑO: se implementan las medidas técnicas y organizativas para proteger los datos personales desde el inicio del diseño de las actividades de procesamiento, de forma que se salvaguarden los principios de privacidad y protección de datos desde el principio

POR DEFECTO: únicamente se procesan los **datos personales necesarios** para el objetivo concreto (datos adecuados, relevantes y limitados). Incluye: la cantidad de datos, las actividades y el período de procesamiento, la accesibilidad.

Anonimización y Pseudonimización



ANONIMIZACIÓN es el proceso por el cual se **eliminan los identificadores personales**, ambos directos e indirectos, que pueden llevar a identificar a un individuo. Cuando los datos están anonimizados y los individuos ya no son identificables, los datos ya no están regulados por el RGPD

PSEUDONIMIZACIÓN: 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

Cultura institucional en protección de datos personales

LA PRIVACIDAD DE LOS PARTICIPANTES EN LOS ESTUDIOS (y otros)

Somos los responsables de manejar la

información **MÁS SENSIBLE** de las personas

Reputación

Compliance

La protección de datos **IMPLICA A TODA** la institución

Investigadores, estadísticos / data managers, legal, gestión de la ciencia, formación, recursos humanos, compras, etc

La protección de datos VA MÁS ALLÁ de la regulación

Vínculos con la **ética**

Vínculos con las iniciativas de **Open** Science

ISGlobal

Ética por diseño

(...) implicar a los investigadores durante la fase de diseño de la propuesta para que las **consideraciones éticas puedan integrarse directamente en la ciencia** en lugar de considerarse como un añadido a posteriori. Esta propuesta de colaboración en el diseño de la investigación tiene como resultado el establecimiento de una cultura de investigación ética en lugar de una investigación con supervisión ética.

La Comisión Europea define la ética por diseño como la aplicación, desde el **principio del proceso**, de los principios éticos y jurídicos.

Metodología, proceso de selección y consentimiento informado, vulnerabilidad de los participantes, protección de datos personales, comunicación de los resultados…

Soporte interno a los investigadores
Acceso a asesores/expertos locales en ética

DS Borrett, H Sampson, A Cavoukian. Research ethics by design: A collaborative research design proposal. Res Ethics 2017, 13:84-91. https://doi.org/10.1177/1747016116673135

ISGlobal

Proceso de consentimiento informado

NO SE TRATA DE UNA FIRMA, SINO DE UN PROCESO

- Voluntario - Retirada;
- Información clara y comprensible (ejemplos, edad, nivel educativo, circunstancias culturales, etc.);
- Tiempo para hacer preguntas (dudas sobre los procedimientos, visitas, implicaciones, etc.);
- Asegurarse, preguntando al participante, de que la información ha sido realmente comprendida;
- Información continua durante el estudio (requerida por el participante o debido a posibles cambios en los procedimientos);
- Debe garantizarse la privacidad;
- El proceso debe estar documentado; debe entregarse una copia al participante.

Modelo de consentimiento informado

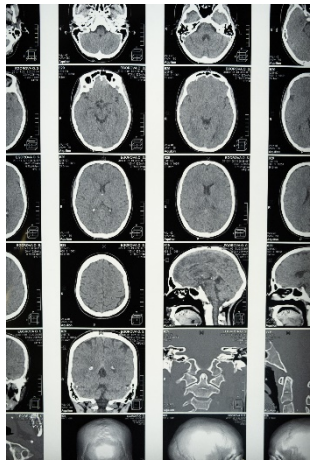
- Finalidad de la investigación: dejar clara la diferencia entre investigación y asistencia
- Diseño y duración del estudio
- Qué hay que hacer
- Alternativas
- Riesgos y beneficios, y cómo se informará a los participantes de los resultados (gestión de hallazgos incidentales)
- Remuneración, compensación
- Seguro (si procede)
- **Protección de datos y confidencialidad:** Quién trata los datos, finalidad (actual y futura), riesgos potenciales, almacenamiento, planes para compartirlos, cómo ejercer los derechos
- Muestras y genética (si procede)

Procesamiento de datos personales & Ética

- Hallazgos incidentales - Acción

- Privacidad de los participantes – Evaluación del riesgo

- Comunicación de los resultados – Evaluación de impacto (*misuse*)

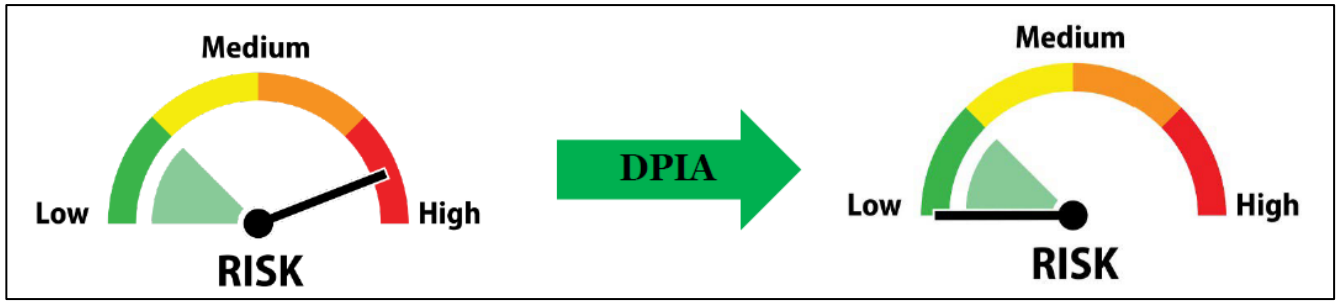


ISGlobal

Otros aspectos éticos relacionados con la protección de datos personales

- Tratamiento posterior de los datos recogidos previamente. Compruebe el consentimiento informado, consulte al Comité de Ética.
- Uso de datos disponibles "públicamente" (por ejemplo, redes sociales): Considerar el uso, los riesgos para los sujetos.
- Las transferencias internacionales:
  - Comprobar la legislación local / nacional.
  - Acuerdo de transferencia de datos, compromiso de no reidentificación
  - Minimización de datos
  - Sistemas de transferencia seguros
  - Análisis federado

Evaluación de impacto relativa a la protección de datos (DPIA)



¿Qué es una evaluación de impacto relativa a la protección de datos?

Una DPIA es un proceso/evaluación cuyo objetivo es identificar los riesgos asociados al procesamiento de datos personales y aplicar medidas para mitigar/reducir al mínimo estos riesgos.

Ver Art. 35 GDPR

Políticas y procedimientos institucionales

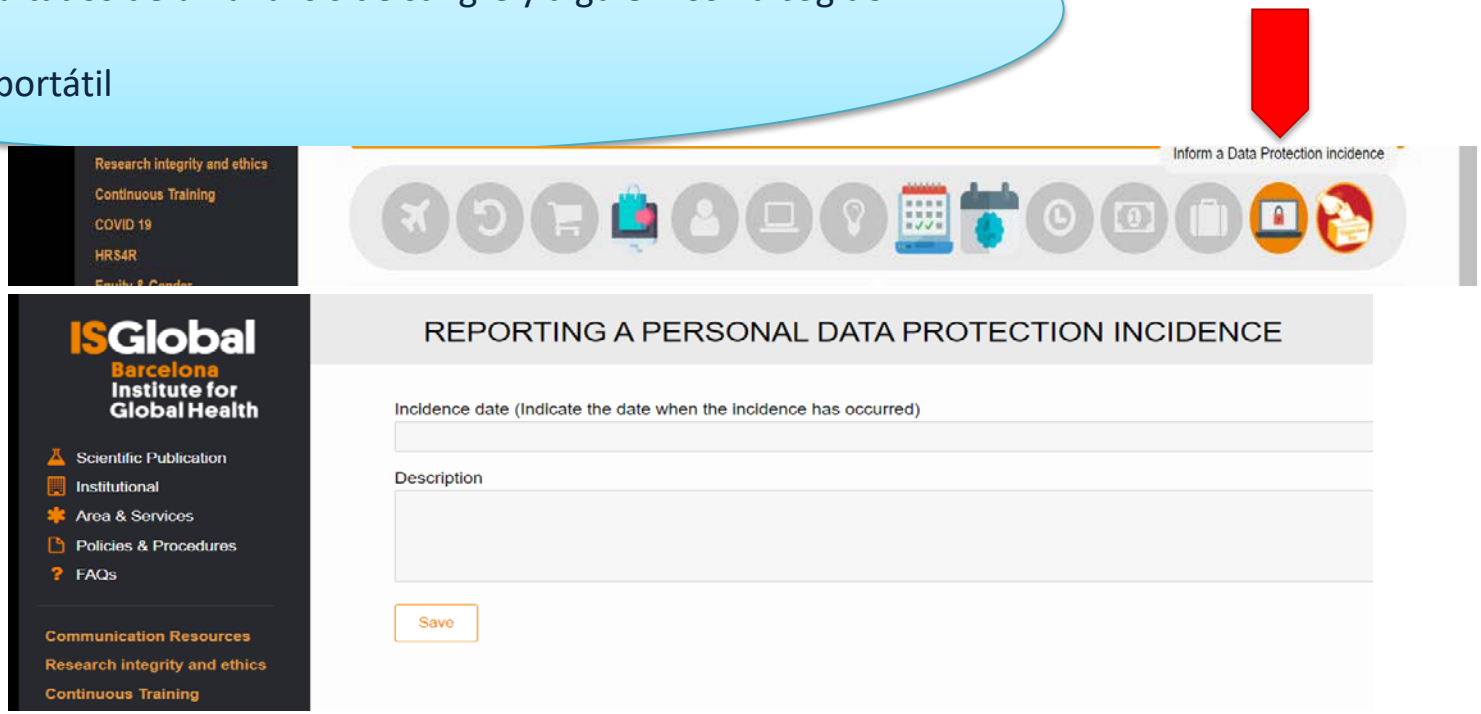
- Código de Buenas Prácticas Científicas (& Addenda)
- ISG-DP-POL-PersonalDataProtection_GDPR v2
- ISG-IT-POL-Rules for the use of ISGlobal IR resources and services v5

Pack de bienvenida y en la intranet

Contacta al DPO: lopd@isglobal.org

Cómo reportar una incidencia de datos personles?

He recibido por correo electrónico un fichero con datos personales
He impreso los resultados de un análisis de sangre y alguien los ha cogido de la impresora
Me han robado el portátil



ATENCIÓN- Las brechas de seguridad deben notificarse a la AEPD en 72 horas

Derechos ARCO POL

Por favor, borren mis datos de la base de datos
No deseo recibir más información de ustedes
Deje de enviarme este boletín
He cambiado de domicilio

- Derecho de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición al tratamiento de sus datos

CRUCIAL: Contacte con el DPO (lopd@isglobal.org) si detecta algún sujeto dispuesto a ejercer estos derechos.

LA RESPUESTA DEBE DARSE EN UN PLAZO MÁXIMO DE 1 MES

Introducción a la privacidad y la seguridad de la información

Ponentes

Cristina Pérez Solà

Ingeniera informática y doctora en informática por la Universidad Autónoma de Barcelona (UAB) y la Katholieke Universiteit Leuven (KULeuven). Actualmente es profesora en la Universitat Oberta de Catalunya, donde coordina asignaturas del área de seguridad y privacidad de los datos y de programación. Su ámbito de investigación es la seguridad y la privacidad, poniendo especial énfasis en datos y sistemas que se pueden moldear como redes. Actualmente, su investigación se centra en el ámbito de las criptomonedas, tanto estudiando la red P2P que las soporta como las redes de pagos que emergen de éstas.

Julián Salas Piñón

Doctor en matemática aplicada por la Universidad Politécnica de Cataluña (UPC). Actualmente es investigador postdoctoral en la Universidad Rovira i Virgili (URV). Su ámbito de investigación es la privacidad de los datos. Actualmente, su investigación se centra en el aprendizaje automático responsable, que procura explicar los modelos de aprendizaje automático, mitigar los sesgos en los modelos y proteger los datos con los que se entrenan. Su investigación incluye métodos de protección de la privacidad de datos de redes sociales, geolocalizadas o de sensores, para generar modelos predictivos y sistemas de recomendación.

Calendario

Jueves 18 de marzo de 9:30 a 11h y 11:30h a 13h.

Objetivos

- Conocer la problemática relacionada con los datos de carácter personal y/o privado.
- Entender las limitaciones de la pseudonimización
- Conocer los principales modelos teóricos de preservación de la privacidad
- Conocer las principales técnicas para aplicar privacidad en datos tabulares
- Entender las propiedades básicas que definen la seguridad de los datos
- Conocer las principales familias de primitivas criptográficas
- Aprender cómo se puede utilizar la criptografía para proteger los datos

A quién va dirigido

Este curso va dirigido a investigadores o personas que trabajan con datos de carácter personal y/ o privados.

Programa

Parte 1: Introducción a la privacidad de los datos (1h + 30 minutos)

1. Problemática de la publicación y compartición de datos
    a. Escenario
    b. Limitaciones de la pseudo-anonimización
2. Modelos teóricos de privacidad
    a. K-anonimidad
    b. Privacidad diferencial
3. Anonimización de datos tabulares
    a. Métodos de enmascaramiento
    b. K-anonimidad en tablas
    c. Privacidad diferencial en tablas
4. Anonimización de otros tipos de datos 5.

Ejemplo práctico / turno de preguntas

Parte 2: Introducción a la seguridad de los datos (1h + 30 minutos)

1. Seguridad de la información
    a. Propiedades básicas de la seguridad de la información
    b. Criptografía y criptoanálisis
    c. Ataques a la seguridad de los datos
2. Introducción a la criptografía de clave simétrica
    a. Cifras de flujo
    b. Cifras de blog
    c. La problemática de la gestión de claves
3. Introducción a la criptografía de clave pública
    a. Cifrado con llave pública
    b. Firmas digitales c. Infraestructura de clave pública
4. Introducción a las funciones hash
    a. Propiedades de las funciones hash
    b. Aplicaciones de las funciones hash
5. Turno de preguntas

Decálogo CiberSeguridad para usuarios de ISGlobal

(1) Acceso a la información (usuario y contraseña): Únicamente **los usuarios autorizados** con acceso al sistema de información **deberán contar con una credencial de acceso** (usuario/contraseña) **única, personal e intransferible**, estando prohibido compartirla con otros. **La contraseña debe seguir un patrón seguro y debe cambiarse regularmente**. Si algún usuario sospecha que su credencial de acceso personal está siendo utilizada por otra persona debe cambiar inmediatamente su contraseña y avisar al Responsable de Seguridad (SRI).

(2) Adquisición y uso de equipos informáticos: Los **equipos informáticos y dispositivos móviles** deben ser adquiridos y gestionados por ISGlobal, y **su uso es exclusivamente profesional dentro de la Institución**. En ningún caso podrán ser utilizados para fines o actividades particulares. Únicamente el personal autorizado de SRI podrá realizar tareas de reparación, instalación o mantenimiento.

(3) Conexiones de red: **Sólo se pueden conectar a la red interna de ISGlobal los equipos informáticos institucionales**, que hayan sido instalados y configurados por SRI. Las computadoras y dispositivos personales solo podrán conectarse a la red de invitados o WiFi, y solo en casos excepcionales podrán conectarse a la red interna bajo la supervisión del personal del SRI, y previa adaptación a las directivas técnicas y de seguridad de la institución.

(4) Uso de Software: **Sólo se podrán instalar en los equipos informáticos de ISGlobal aplicaciones y software legalmente utilizables**, con la correspondiente **licencia y adquiridos por ISGlobal**, o aplicaciones con licencias de uso libre que SRI haya aprobado previamente

(5) Dispositivo extraviado o sustraído (Protección de Datos): Para todos los equipos informáticos y dispositivos móviles, **en caso de pérdida o robo**, se deberá comunicar de forma inmediata (en un plazo máximo de 24 horas) **a los responsables de seguridad,** personal del DPO y del SRI, y debe cambiar la contraseña de su cuenta lo antes possible.

(6) Inicio de sesión y conexiones a Internet: Para todos los equipos y dispositivos de red, **todas las sesiones serán cerradas o bloqueadas con contraseña**, en el caso de **ausencia temporal del trabajo.** Al final de la jornada laboral, los **equipos informáticos deberán estar apagados**, excepto aquellos equipos que estén realizando alguna tarea que requiera que permanezcan encendidos (en cuyo caso se deberá notificar al SRI). No navegue por **páginas web "peligrosas",** ni haga **click en enlaces** recibidos de origen dudoso

(7) Almacenamiento y Backup de Datos: **Todos los datos propiedad de ISGlobal, deberán ser almacenados en los servidores de la Institución**, dentro de un repositorio interno de la red debidamente protegido, para garantizar la integridad y seguridad de esta información. **Los usuarios se obligan a proteger toda esta información,** impidiendo el acceso externo no autorizado.

(8) Envío de Información: **Los datos personales nunca deben ser enviados a través de redes inalámbricas públicas o externas** (incluso por correo electrónico), y **es obligatorio codificar los datos o utilizar cualquier otro método de encriptación, con protocolos seguros de transferencia de datos** proporcionados por SRI, que garantizan que la información no sea inteligible o manipulada por terceros.

(9) Uso de Gmail (Phishing y Spam): Todos los empleados de ISGlobal **deben utilizar las Apps de Google Suite institucional** (Gmail, GDrive, y otras Google Apps...) **para un uso**

estrictamente profesional. Gmail no debe utilizarse para: enviar o transferir información confidencial de datos personales sin la autorización previa del DPO y el soporte de IT, y tampoco debe usarse para enviar correos electrónicos masivos para evitar problemas de spam. **No responda a correos electrónicos de remitentes desconocidos** (¡compruebe la dirección!). Especial atención a los **correos electrónicos sospechosos** con solicitudes de información confidencial o personal, **para evitar phishing**. Cualquier duda, contactar con SRI.

(10) Acceso remoto : Las conexiones externas a los servicios y recursos de la red de ISGlobal **deben realizarse siempre a través de una conexión VPN remota segura**, y **utilizando equipos o dispositivos institucionales** proporcionados por la institución y gestionados por el personal del SRI. Una vez finalizada la jornada laboral, en la situación de movilidad o teletrabajo, deberás desconectar la sesión de acceso remoto (VPN) y apagar o bloquear el acceso al dispositivo.

***** *Source: Rules for the Use of ISGlobal IT Resources and Services*
(can be found in the Intranet Section > Policies & Procedures > SRI Documents)

De: Joana Porcel
A: LOPD Working Group
Cc: Everyone
Asunto: PERSONAL DATA PROTECTION - UPDATE (Please review carefully)
Fecha: miércoles, 7 de julio de 2021 12:17:12

On behalf of the WG on Personal Data Protection

Dear all,

Hope you are fine.

Here's an update on the personal data protection advances in the last months:

- ***Updated policies in the context of TELEWORKING AND MOBILITY situations***. The Personal Data Protection Policy and the Rules for the Use of ISGlobal IT Resources and Services have been updated, following the indications of the Spanish Agency for Data Protection, to include an Annex with the specific recommendations for teleworking and mobility situations. The documents are available at the intranet, please read them carefully and contact us if you have any question.

- ***A leaflet and a video*** – We have prepared a LEAFLET-TELEWORKING and a VIDEO with the most relevant issues to be considered in the context of teleworking or mobility situations. Hope you find them useful to remind the main recommendations.

- ***Data Protection Audit*** – In October 2020, we had the external personal data audit with the external reviewers who interview several people to check how we are processing personal data and which are our main concerns. Many thanks to all the participants. As usual, the auditors made a number of recommendations that are implemented and closely monitored by the WG on DP.

- ***DP Training*** – The training on personal data protection has been adapted to the current teleworking situation. If you are processing sensitive data in a complex project, please let us know, and we'll organize a project-specific training with your team.

- ***Data Protection Impact Assessment (DPIA)*** – We are working on a DPIA template to facilitate a project-specific assessment in case the funding agency requires so. We'll keep you inform on this in the following months.

Other **RELEVANT** issues to remind:

- Intranet form to ***COMMUNICATE ANY PERSONAL DATA INCIDENCE***. "I've lost my cell phone; I've found printed documents with personal data at the printer; My laptop has been stolen…" These are examples of incidences that must be reported. You could do that through the FORM AT THE INTRANET, click on the logo and briefly describe what has happen. We will contact you for review and follow-up.

- Checklist ***Are you compliant with data protection***. Hope you find this information

useful, it summarizes the principal measures to protect the personal data that we are managing. You can find the LEAFLET- CHECKLIST at the intranet , together with the complete policies on Data Protection and IT use of resources. The leaflets is also placed in the common areas.

All of us are responsible of managing the people's most sensitive information, and we must guarantee the study participants' privacy. If you have any question or doubt please contact us (lopd@isglobal.org)

Have a very nice and relaxing summer break,

Joana

Joana Porcel

Research Manager

Data Protection Officer

Head of the Projects Unit

ISGlobal

Campus MAR, Barcelona Biomedical Research Park (PRBB)

Doctor Aiguader, 88 - Hipàtia, 08003 Barcelona, Spain

Tel. +34 93 214 73 70

ISGlobal

Campus Clínic, Hospital Clínic - Universitat de Barcelona

Rosselló, 132, 5º 2ª, 08036 Barcelona, Spain

joana.porcel@isglobal.org

www.isglobal.org

En nombre del GT de Protección de Datos Personales

Estimados,

Aquí una actualización sobre los avances en protección de datos personales en los últimos meses:

- Políticas actualizadas en el contexto de situaciones de TELETRABAJO Y MOVILIDAD. Se ha actualizado la Política de Protección de Datos Personales y las Normas de Uso de los Recursos y Servicios Informáticos de ISGlobal, siguiendo las indicaciones de la Agencia Española de Protección de Datos, para incluir un Anexo con las recomendaciones específicas para situaciones de teletrabajo y movilidad. Los documentos están disponibles en la intranet, léalos atentamente y contáctenos si tiene alguna pregunta.

- Un folleto y un vídeo – Hemos elaborado un FOLLETO-TELETRABAJO y un VÍDEO con las cuestiones más relevantes a considerar en el contexto de situaciones de teletrabajo o movilidad. Espero que os resulten útiles para recordar las principales recomendaciones.

- Auditoría de Protección de Datos – En octubre de 2020 realizamos la auditoría externa de datos personales con los revisores externos que entrevistan a varias personas para comprobar cómo estamos procesando los datos personales y cuáles son nuestras principales preocupaciones. Muchas gracias a todos los participantes. Como es habitual, los auditores formularon una serie de recomendaciones que el Grupo de Trabajo sobre PD implementa y supervisa de cerca.

- Formación DP – Se ha adaptado la formación en protección de datos personales a la situación actual del teletrabajo. Si está procesando datos confidenciales en un proyecto complejo, háganoslo saber y organizaremos una capacitación específica del proyecto con su equipo.

- Evaluación de impacto de la protección de datos (DPIA): estamos trabajando en una plantilla de DPIA para facilitar una evaluación específica del proyecto en caso de que la agencia de financiación así lo requiera. Os mantendremos informados sobre esto en los próximos meses.

Otras cuestiones RELEVANTES para recordar:

- Formulario de intranet para COMUNICAR CUALQUIER INCIDENCIA EN DATOS PERSONALES. “Perdí mi celular; He encontrado documentos impresos con datos personales en la imprenta; Me han robado el portátil…” Estos son ejemplos de incidencias que hay que denunciar. Puedes hacerlo a través del FORMULARIO EN LA INTRANET, pinchar en el logo y describir brevemente lo sucedido. Nos comunicaremos con usted para revisión y seguimiento.

- Lista de verificación ¿Cumple con la protección de datos? Espero que encuentres esta información. De gran utilidad, resume las principales medidas para proteger los datos personales que estamos manejando. Puede encontrar el FOLLETO-CHECKLIST en la intranet, junto con las políticas completas sobre Protección de Datos y uso de recursos TI. Los folletos también se colocan en las zonas comunes.

Todos somos responsables de gestionar la información más sensible de las personas, y debemos garantizar la privacidad de los participantes del estudio. Si tiene alguna pregunta o duda por favor contáctenos (lopd@isglobal.org).

ISGlobal
Barcelona
Institute for
Global Health

Protocolo ante el robo o hurto de equipos propiedad de ISGlobal

Acciones a realizar

PROTOCOLO

ISGlobal

1.- Comunicar los hechos a través del formulario de incidencias de protección de datos de la Intranet

(https://isg-intranet.isglobal.org/data_protection_issues/new

Responsable: La comunicación debe realizarla el **afectado** siempre que sea empleado/a o colaborador/a de ISGlobal. En caso de que los hechos estén relacionados con un equipo cedido a voluntarios/as de proyectos o estudios, la incidencia debe realizarla el/la **PM** o quien designe el/la **IP del proyecto**.

2.- Formular la denuncia de los hechos ante las Fuerzas y Cuerpos de Seguridad del Estado (v.g. Mossos d'Esquadra)

Responsable: **Usuario** afectado o, en su defecto, **apoderado** de ISGlobal**.**

PROTOCOLO

ISGlobal

3.- Notificar los hechos a la AEPD en el plazo máximo de 72 horas, siempre y cuando ello constituya una "brecha de seguridad".

Responsable: Delegada de Protección de Datos (**DPO**) y su equipo de soporte.

4.- Solicitar al proveedor de servicios de Internet la baja de la línea telefónica/datos asociada al equipo (cuando el equipo disponga de ella)

Responsable: Departamento de **Compras.**

5.- Dar de baja el equipo a nivel contable/inventario (activo fijo)

Responsable: Departamento de **Contabilidad y de SRI.**

6.- Hacer seguimiento de la incidencia hasta su cierre e implementar las medidas de seguridad adicionales en caso de que resulten necesarias.

Responsable: Delegada de Protección de Datos (**DPO**) y su equipo de soporte.

PROTOCOLO

ISGlobal

1.- Comunicar los hechos a través del formulario de incidencias de protección de datos de la Intranet

2.- Formular la denuncia de los hechos ante las Fuerzas y Cuerpos de Seguridad del Estado (v.g. Mossos d'Esquadra)

3.- Notificar los hechos a la AEPD en el plazo máximo de 72 horas, siempre y cuando ello constituya una "brecha de seguridad".

4.- Solicitar al proveedor de servicios Internet la baja de la línea telefónica/datos asociada al equipo (cuando el equipo disponga de ella)

5.- Dar de baja el equipo a nivel contable/inventario (activo fijo)

6.-Hacer seguimiento de la incidencia hasta su cierre e implementar las medidas de seguridad adicionales en caso de que resulten necesarias.

ISGlobal

MODELO DE HOJA DE INFORMACIÓN DEL PARTICIPANTE Y CONSENTIMIENTO INFORMADO

Barcelona, 17 January 2022

Modelo de Hoja de Información del Participante y Consentimiento Informado (HIP / CI)	**Date** 17 January 2022	**Prepared by** Research Manager

ESTE MODELO:

Esta es una plantilla para preparar la Hoja de Información y el Formulario de Consentimiento para su proyecto. El documento está en español, pero debe prepararse en un idioma y términos comprensibles para los participantes en el estudio.

Para poder tomar decisiones con conocimiento de causa, los participantes tienen derecho a: conocer los detalles del proyecto al que se les ha invitado a participar y por qué se les ha invitado; saber que su participación es voluntaria y que pueden retirarse en cualquier momento sin dar explicaciones; hacer preguntas y recibir respuestas comprensibles antes de tomar una decisión; conocer el grado de riesgo y la carga que supone la participación; saber quién se beneficiará de la participación. También se informará a los participantes de sus derechos en materia de protección de datos personales.

En el caso de menores (o personas legalmente incapacitadas), el consentimiento debe obtenerse de los padres / tutores legales y el asentimiento (utilizando un formulario de asentimiento adaptado al menor y escrito en un estilo fácilmente comprensible) debe obtenerse del menor.

En caso de que tenga previsto realizar un análisis genético, deberá preparar un formulario de consentimiento por separado; encontrará la información, incluido cómo comunicar los resultados, en la sección de muestras de esta plantilla.

El HIP / CI debe ser aprobado por el comité ético correspondiente antes de iniciar el reclutamiento de los participantes.

Formato: el HIP / CI debe ser un documento independiente del protocolo. Debe incluir la versión, la fecha y el número de página.

Revise las Guías Europeas sobre consentimiento informado: https://ec.europa.eu/research/participants/data/ref/fp7/89807/informed-consent_en.pdf

Modelo de Hoja de Información del Participante y Consentimiento Informado (HIP / CI)	Date 17 January 2022	Prepared by Research Manager

HOJA DE INFORMACIÓN DEL ESTUDIO XXXXX

Versión y fecha:

TÍTULO DEL ESTUDIO:

INVESTIGADOR PRINCIPAL:

Introducción

You need to explain that you are asking the participant to take part in research, and explain very briefly the study.

Esta hoja informativa proporciona detalles de un proyecto de investigación sobre XXXXX *(indicate the area of research)* en el que le proponemos participar. Por favor, tómese tiempo para leer esta información detenidamente y haga todas las preguntas que considere. Antes de decidir si participan, puede consultar con las personas que considere oportuno.

Usted ha sido invitado a participar porqué XXXX *(explain briefly why and how the participant was chosen and how many others will be in the study. For example, explain clearly why you have chosen to recruit participants within a particular age group, healthy volunteers, students on a particular course, males or females and why you are studying this particular population group.).*

El estudio se lleva a cabo por parte del Instituto de Salud Global Barcelona *(add others if apply).* Este estudio ha sido aprobado por el Comité de Ética del (*select and add others if apply,* Hospital Clínic / PS Mar), de acuerdo a la legislación vigente (Ley de Investigación Biomédica 14/2007).

Su participación es voluntaria

Su participación en este estudio es totalmente voluntaria. Usted puede decidir participar o no en el mismo. Asimismo, puede cambiar su decisión y retirar el consentimiento en cualquier momento del estudio, sin que tenga que dar ninguna explicación (*this must be added in clinical studies:* y sin que por ello se altere la relación con su médico ni se produzca perjuicio alguno en su tratamiento).

Si usted decide retirar el consentimiento para participar en este estudio, no se añadirán datos nuevos en la base de datos a partir de la fecha en que nos comunique que decide retirarse, y se mantendrán únicamente los datos obtenidos hasta ese momento, para garantizar la validez de la investigación.

(add in case biological samples are collected) Usted puede pedir que las muestras biológicas identificables obtenidas hasta el momento sean destruidas, de manera que no puedan realizarse nuevos análisis.
Le informamos también que podría ser excluido del estudio si el promotor y/o los investigadores del estudio lo consideran oportuno, ya sea por motivos de seguridad, por cualquier acontecimiento adverso que se produzca y se considere relacionado con su participación en el estudio o porque consideren que no está cumpliendo con los procedimientos establecidos. En cualquiera de los casos, si esto ocurre, le explicaremos el motivo que ha ocasionado su retirada del estudio.

¿En qué consiste el estudio y su participación en el mismo?

This section should include:

- *how long the participant will be involved in the research*
- *how long the research will last (if different)*
- *how often they will need to attend, meet a researcher,*
- *how long these visits will be*
- *what exactly will happen, for example: procedures, tests, questionnaires, interviews, discussion groups....*

Use the most appropriate format to demonstrate their involvement. Add diagrams/tables/images, if necessary. The detail will depend on the complexity of the study. It may help if the information is displayed in a flow chart or grid indicating what will happen at each visit, where appropriate.
If the study will involve video/audio-taping or photography, you should explain what is intended, including the confidentiality issues. Specific consent will be needed if material of any sort will be published that identifies the subject. ***IMP.*** *If you plan to do so, the personal data protection clause must be adapted accordingly.*

Expected length 1-3 pages

Modelo de Hoja de Información del Participante y Consentimiento Informado (HIP / CI)	Date 17 January 2022	Prepared by Research Manager

¿Cómo vamos a tratar sus muestras biológicas?

This section must be included if biological samples (regardless the type of sample) are collected.

Para responder a los objetivos del estudio, necesitamos obtener muestras de *(specify the type of samples that you plan to collect: blood, saliva, nails, etc.)*. De acuerdo a la legislación vigente (Ley 14/2007 de investigación biomédica; Real Decreto 1716/2011 por el que se regula la utilización de muestras biológicas en investigación), al firmar este documento usted acepta que se utilicen las muestras que se obtendrán para los objetivos de este estudio: *(describe the use of the samples according to the study aims).*

Las muestras se mantendrán almacenadas en *(specify where the samples will be stored)* hasta su utilización para los objetivos de este estudio. Una vez finalizado, las muestras sobrantes serán

- destruidas *(select this option, in case samples are only collected for this study. This means that the samples CANNOT be used for other aims or future studies but the ones of this study)*
- almacenadas en la colección *(include the collection reference number from the Registro de Colecciones del ISCIII; https://biobancos.isciii.es/ListadoColecciones.aspx)* para estudios en *(specify the Research line of the collection. **IMPORTANT** for checking the current ISGlobal collections or Registering a new collection, contact Laura Puyol – Campus Clínic; Lourdes Arjona – Campus Mar)*

*(**NOTE**: according to the Spanish law, samples can also be stored at a legal biobank. If you plan to do so, please contact Laura Puyol – Campus Clínic / Lourdes Arjona – Campus Mar, as this requires a specific procedure and an agreement with the IDIBAPS / MAR Biobanks).*

Sus muestras serán identificadas con un código, de manera que no podrán desvelar su identidad. Únicamente el investigador del estudio y sus colaboradores podrán relacionar la muestra con usted.

Los datos que se obtengan de la utilización de estas muestras se tratarán del mismo modo que el resto de datos que se obtengan en este estudio.

La cesión de muestras biológicas para este estudio es gratuita y voluntaria. Esto supone que usted no tendrá derechos sobre posibles beneficios comerciales de los descubrimientos que pudieran derivarse del resultado de la investigación biomédica.

Si se obtuviera información relevante que pudiera afectar a su salud o a la de sus familiares, se le notificará. En caso que fuera necesario contactar con usted, se utilizarían los datos que nos haya facilitado. No obstante, se respetará su derecho a decidir que no se le comuniquen éstos, para lo que puede marcar la casilla que se encuentra en el formulario de consentimiento.

*(**For genetic studies,** and according to the current regulation, the following information must be provided: aim of the genetic analysis, expected benefits, potential discomfort during the simple donation, place where the analysis is going to be conducted, who will have access to the results, information about the possibility of incidental findings and how this will be managed, the right to know / not to know, and how to contact them or their relatives according to the regulation, the commitment to provide genetic counselling, the right to withdrawn consent and to request the samples' destruction – if not anonymised)*

Las muestras biológicas y el ADN y ARN extraídos de ellas se almacenarán en los laboratorios XXXX. Las muestras se integrarán en la colección XXXX registrada en el Registro de Colecciones del Instituto de Salud Carlos III para investigación en XXXX. *(alternatively, samples could be obtained only for this project and then destroyed, or stored at a legal biobank. Storing the samples at a "legal" biobank requires the specific consent form of the biobank).*

Para analizar el genoma/epigenoma/transcriptoma/..., las muestras podrán ser enviadas a laboratorios colaboradores. Siempre que se envíen muestras a laboratorios colaboradores se seguirá la normativa vigente y se firmará un acuerdo para garantizar su anonimato y el uso de las muestras solamente para los objetivos del proyecto.

Las muestras biológicas y el ADN y ARN restante se almacenarán de forma segura para futuros estudios relacionados con XXXX en los laboratorios de XXXX.

- **¿Cómo le comunicaremos los resultados de los análisis genéticos?**

El estudio no tiene como objetivo identificar variantes genéticas asociadas a una predisposición alta a sufrir algún tipo de enfermedad, por lo tanto, no proporcionarán información útil para el diagnóstico de enfermedades. Sin embargo, siguiendo la normativa legal vigente, en el caso de que detectemos un hallazgo genético que tenga implicaciones para su salud, se lo podremos comunicar si así lo ha indicado en el formulario del consentimiento.

En caso de querer ser informado el circuito que seguiremos será el siguiente: *(you need to define a procedure for communicating the relevant results to the participants, usually this is managed through the genetic services of the hospitals).*

Modelo de Hoja de Información del Participante y Consentimiento Informado (HIP / CI)	Date 17 January 2022	Prepared by Research Manager

En caso de no querer ser informada/o, y de acuerdo con la legislación vigente, si el especialista de XXXX *(include the name of the hospital)* considere que el hallazgo puede tener implicaciones graves para la salud de sus familiares biológicos, igualmente nos pondremos en contacto con usted, para así poder contactar con sus familiares.

(this is the text of the current Spanish legislation that regulates the communication of genetic results to the study participants: La comunicación de los resultados genéticos se hará de acuerdo al Artículo 4.5 de la Ley 14/2007, de 3 de julio, de Investigación biomédica (https://www.boe.es/eli/es/l/2007/07/03/14) "Toda persona tiene derecho a ser informada de sus datos genéticos y otros de carácter personal que se obtengan en el curso de una investigación biomédica, según los términos en que manifestó su voluntad. El mismo derecho se reconoce a la persona que haya aportado, con la finalidad indicada, muestras biológicas, o cuando se hayan obtenido otros materiales biológicos a partir de aquéllos. Se respetará el derecho de la persona a decidir que no se le comuniquen los datos a los que se refiere el apartado anterior, incluidos los descubrimientos inesperados que se pudieran producir. No obstante, cuando esta información, según criterio del médico responsable, sea necesaria para evitar un grave perjuicio para su salud o la de sus familiares biológicos, se informará a un familiar próximo o a un representante, previa consulta del comité asistencial si lo hubiera. En todo caso, la comunicación se limitará exclusivamente a los datos necesarios para estas finalidades.).

¿Cómo vamos a tratar sus datos personales y garantizar su confidencialidad?

*(this text **CANNNOT** be modified, you can complete / adapt according to the project)*

Los datos se tratarán con absoluta confidencialidad y de acuerdo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

Los datos de salud se mantendrán disociados de los datos personales. Disociar los datos significa que su información de salud no podrá asociarse a usted ya que sus datos personales identificativos (nombre, apellidos, etc.) se sustituyen por un código. La información disociada se archivará para ser usada por investigadores del proyecto y sus socios de investigación. Todos los resultados del estudio serán presentados en una base de datos del grupo de participantes, nunca se presentarán datos de forma individual *(In some studies, for instance opinion surveys from experts, the name of the respondent could be published. If this is the case, specific consent must be obtained and this text must be adapted).*

Modelo de Hoja de Información del Participante y Consentimiento Informado (HIP / CI)	Date 17 January 2022	Prepared by Research Manager

A continuación, le detallamos la información sobre la protección de datos personales, por favor léala detenidamente y consúltenos si tiene alguna duda:

- **¿Quién es el responsable del tratamiento de sus datos personales**

Responsable del Tratamiento: Fundación Privada Instituto de Salud Global Barcelona (ISGlobal), CIF: G65341695, Dirección postal: Calle Rosselló, número 132, 6ª de Barcelona (08036). Delegado de Protección de Datos, contacto: lopd@isglobal.org

- **¿Con qué finalidad tratamos sus datos personales?**

De acuerdo a su participación en el proyecto de investigación *(indicate the title of the study and a very short description, you can include the same description as in the Introducción)*, el Responsable del Tratamiento le informa que, en cumplimiento de lo establecido en el Reglamento General de Protección de datos y la Ley Orgánica 3/2018, sus datos de carácter personal serán utilizados, para llevar a cabo la investigación a la que usted ha consentido participar.

(in case, your project requires to geo-localised the participants, the following text must be included)
De igual manera, el tratamiento de sus datos también incluirá su geolocalización, a partir del captador personal entregado, durante unos días que serán determinados en su momento con la intención de poder realizar mediciones ambientales en los espacios y localizaciones en los que desarrolla su vida cotidiana.

Asimismo, es importante informarle que los datos de carácter personal, si usted otorga su consentimiento, podrán serán utilizadas por otros proyectos / investigaciones dentro del área del presente proyecto, o bien en proyectos de investigación en salud global, tanto en enfermedades infecciosas como no-comunicables, y salud ambiental, para estudiar el efecto de los factores ambientales en la salud de las personas.

Sus datos personales no serán utilizados para elaborar perfiles ni la toma de decisiones automática.

- **¿Cuál es la legitimación para el tratamiento de sus datos personales?**

La base legal para el tratamiento de datos es el consentimiento que usted ha proporcionado mediante la aceptación de la cláusula de tratamiento de datos. La obtención de sus datos es necesaria para llevar a cabo el proyecto de investigación sin las cuales no podría realizarse, sin perjuicio de que usted en cualquier momento tiene derecho a retirar los consentimientos prestados, sin que esto afecte la licitud del tratamiento realizado previamente a su retirada.

- **¿Por cuánto tiempo conservaremos sus datos personales?**

a- (select this option in non-clinical trials) Los datos proporcionados serán conservados mientras esté en activo el proyecto de investigación o bien los sucesivos proyectos de investigación dentro de la misma área o línea de investigación en los que se traten sus datos de carácter personal, de acuerdo a los criterios que establezca la legislación vigente.

b- (select this option for clinical trials) El Investigador y el Promotor están obligados a conservar los datos recogidos para el estudio al menos hasta 25 años tras su finalización. Posteriormente, su información personal solo se conservará por el centro para el cuidado de su salud y por el promotor para otros fines de investigación científica si usted hubiera otorgado su consentimiento para ello, y si así lo permite la ley y requisitos éticos aplicables.

- **¿A qué destinatarios se comunicarán sus datos personales?**

Esta información será utilizada por el Grupo de Investigación encargado de la investigación *(in case the data is being collected in the framework of a collaborative project, the following can be included)*, en particular por los socios del proyecto XXXX *(add website, if available),* que están ubicados en países europeos o países que tienen un nivel adecuado de protección de datos personales.

Para transferencias a terceros países, sólo se cederán los datos codificados, que en ningún caso contendrán información que pueda identificarle directamente (por ejemplo, nombre y apellidos, iniciales, dirección, número de la seguridad social, etc.). En el supuesto de que se produjera esta cesión, sería para las mismas finalidades descritas en este documento y garantizando la confidencialidad.
Si se realizara una transferencia de datos codificados fuera del Espacio Económico Europeo, ya sea a entidades relacionadas con el centro donde usted participa, a prestadores de servicios o a investigadores que colaboren con nosotros, sus datos quedarán protegidos por salvaguardas como contratos u otros mecanismos establecidos por las autoridades de protección de datos.

Los datos personales también podrán ser comunicados a las autoridades sanitarias y el personal de seguimiento y auditoría del patrocinador; todos ellos sujetos a la obligación de secreto profesional en relación con la validación de los datos y procedimientos del estudio, y obligados a mantener siempre esta confidencialidad de acuerdo con la legislación pertinente. La información también podrá ser compartida con establecimientos oficiales públicos o privados que requieran acceso a los datos, por responsabilidad o necesidad de cumplimiento, con el propósito de la buena conducción del proyecto de investigación, y de acuerdo a las buenas prácticas científicas.

Los datos obtenidos se podrán publicar en repositorios científicos destinados a compartir información entre investigadores con el fin de acelerar la investigación. En caso que se compartan los datos a través de repositorios, se seguirá un criterio de minimización, es decir, se limitará la información compartida y se garantizará su anonimato evitando la publicación de datos que pudieran identificarle.

- **¿Cuáles son sus derechos cuando nos facilita sus datos personales?**

Usted es el responsable de la veracidad y corrección de los datos que nos entrega y tiene la facultad de ejercer los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y de oposición de sus datos de acuerdo lo dispuesto en la normativa en materia de protección de datos. Para ejercerlos, deberá dirigirse por escrito al

Modelo de Hoja de Información del Participante y Consentimiento Informado (HIP / CI)	Date 17 January 2022	Prepared by Research Manager

Delegado de Protección de Datos a lopd@isglobal.org en cualquier caso se deberá adjuntar una fotocopia de su documento nacional de identificación o bien equivalente.
Por último, además de la posibilidad de ejercer sus derechos, si no está de acuerdo con el tratamiento realizado por la Entidad o considera infringidos sus derechos podrá presentar una reclamación en todo momento ante la Agencia Española de Protección de datos.

WORKING WITH ANONYMISED DATA

NOTE: *If you do not need to collect any personal data that make the participant identifiable (name, medical number, ID number, contact details, etc.), this means that you are working* ***with anonymised data*** *(participants cannot be identified, nor contacted in the future, and data cannot be link with other sources), which do not fall under GDPR. Therefore, this clause can be omitted and you only need to inform the participant that:*

En este estudio no vamos a obtener datos personales que permitan identificarle, de manera que toda la información que obtengamos será anónima en todo momento.

¿Cuáles son los beneficios y riesgos de participar en este estudio?

Usually, there are no direct benefits for the study participants, but their contribution to the advancement of knowledge and a more general benefit to the society.

La participación en este estudio no supone un beneficio directo para su salud. La ventaja principal de formar parte es que nos ayudará a entender mejor XXXX. Estos estudios son relevantes ya que aportan evidencia científica sobre XXXX, y con ello se elaboran nuevas políticas *(adapt according to the project).*

(Also describe the potential risks for participating in the project associated with the procedures that will be conducted, i.e. blood drawn, MRI, using a device, etc.)

If applies, include the information of the insurance (this is mandatory for clinical trials, please check).

¿Hay algún tipo de compensación económica por el hecho de participar en el estudio?

If you plan to include a financial compensation (including a voucher), check first with the "assessor the cartera", if this concept is eligible in your project and how to manage it. The amount must be appropriate and not induce coercion. Once approved by the ethics committee, it cannot be changed without submitting an amendment to the committee.

Modelo de Hoja de Información del Participante y Consentimiento Informado (HIP / CI)	Date 17 January 2022	Prepared by Research Manager

¿Cómo se tratarán posibles hallazgos incidentales?

Un "hallazgo incidental" se define como cualquier hallazgo asociado a una prueba, actividad o procedimiento realizado en un proyecto de investigación, que está fuera del ámbito de la investigación, es decir, que no tiene relación con los propósitos, objetivos o variables del estudio.
Le informamos que los procedimientos / test / pruebas / cuestionarios que vamos a utilizar en este estudio se utilizan con el objetivo / tienen la capacidad de diagnosticar enfermedades / trastornos.

Aun así, podría darse la situación que los procedimientos utilizados den lugar a algún hallazgo médico incidental derivado de unos valores anormales en las examinaciones clínicas, XXXX. En caso de encontrar algún resultado que pudiera tener un impacto en su salud (o en la salud de su hijo / a), y siempre y cuando desee ser conocedores de los resultados, le serían comunicados a través de XXXX las enfermeras y sería derivado al especialista pertinente *(describe the process according to the project)*.

¿Cómo se comunican los resultados del estudio?

Los resultados individuales no se comunican de forma rutinaria, a no ser que usted lo indique. Los resultados agregados, es decir, sin que se pueda identificar a las personas individuales que han participado, se publicarán en revistas científicas.
(if you plan to prepare a newsletter or other information tool, you could also inform the participants)
Note: *specific consent must be requested in case you consider to publish an image / voice, or include the name of a participant, for example, to acknowledge someone that have provided an opinion. See personal data protection section.*

¿A quién puede contactar para solicitar más información?

Si desea más información sobre el estudio, por favor contacte con:
(add the contact details, you can also add a webpage with extra information about the study)

Al firmar la hoja de consentimiento adjunta, se compromete a cumplir con los procedimientos del estudio que se le han expuesto. Gracias por leer esta hoja informativa y tener en consideración participar en este estudio.

Modelo de Hoja de Información del Participante y Consentimiento Informado (HIP / CI)	**Date** 17 January 2022	**Prepared by** Research Manager

CONSENTIMIENTO INFORMADO DEL ESTUDIO XXXXX

(you have to prepare two copies: one for the participant and one for the researcher)

Versión y fecha:

TÍTULO DEL ESTUDIO:

INVESTIGADOR PRINCIPAL:

Yo, *(nombre y apellidos del participante)* _____

- He leído la hoja de información que se me ha entregado sobre el estudio.
- He podido hacer preguntas sobre el estudio.
- He recibido suficiente información sobre el estudio.
- Me han informado que el estudio ha sido aprobado por el Comité de Ética XXXX.
- He hablado con: *(nombre del investigador / persona responsable del reclutamiento)* _____
- Comprendo que mi participación es voluntaria.
- Comprendo puedo retirarme del estudio en cualquier momento y sin necesidad tener que dar explicaciones y, sin que ello repercuta en mi atención médica o mis derechos legales.

- De conformidad con lo que establece el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, declaro haber sido informado la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

Ante la presente información que el Responsable del Tratamiento me ha otorgado, y habiendo entendido ésta, ofrezco mi consentimiento al tratamiento de:

☐ Mis datos personales para llevar a cabo el proyecto de investigación.

☐ Mis datos personales para llevar a cabo proyectos de investigación afines al presente o de la misma área de investigación.

☐ Mis datos de geolocalización para llevar a cabo el proyecto de investigación *(add in case participants are going to be geo-localised)*

Modelo de Hoja de Información del Participante y Consentimiento Informado (HIP / CI)	**Date** 17 January 2022	**Prepared by** Research Manager

Deseo que me comuniquen la información derivada de la investigación que pueda ser relevante para mí salud:

SÍ	
NO	

Deseo que me comuniquen los resultados de los análisis genéticos que puedan ser relevante para mí salud:

SÍ	
NO	

Presto libremente mi conformidad para participar en el estudio.

Firma de la participante	Firma del investigador / responsable del reclutamiento

Lugar y fecha: _____

ISGlobal Barcelona Institute for Global Health | EXCELENCIA SEVERO OCHOA | Institució CERCA Centres de Recerca de Catalunya

www.isglobal.org

Institutional Culture on Personal Data Protection

An encompassing approach

Joana Porcel
Aleix Cabrera
Ramon Cifuentes
Paco Fernández

Contact information
joana.porcel@isglobal.org

Protection of personal data (POPD) is a building block of research institutions, especially in those focused on biomedical research.

Centres must guarantee the study participants' privacy, as we are managing the people's most sensitive information.

Researchers require continued and expert advice to manage their projects' needs in terms of personal data protection.

Beyond the Regulation

Broader perspective rather than an isolated issue.

Linked with the ethical and open science implications of the projects.

Institutional Working Group

Including: Research Manager / DPO, the Legal Manager, the IT Manager and members representing the areas of HR, Communication, Statistics, Training and Purchasing.

Monitoring & Reporting System

Including: Direction Committee, Scientific Committee, Compliance Committee and the Administration.

Linking the POPD requirements to the institutional, scientific, compliance and administration policies and procedures.

Implementation

- Continuous support
- Continuous training and debate activities
- External assessments and audits
- Specific material (leaflets and videos), and tools to facilitate POPD management (incidences reporting system, templates - DPIA, informed consent form, protocols, etc.)

This publication is part of project (RCT2020-010666), funded by Spanish Ministry of Science and Innovation (MCIN/AEI/10.13039/501100011033) and European Union "NextGenerationEU"/PRTR

Cultura Institucional en Protección de Datos Personales – Un enfoque integral

Autores: J Porcel, A Cabrera, R Cifuentes, P Fernández

La protección de datos personales (POPD) es un componente básico de las instituciones de investigación, especialmente en aquellas centradas en la investigación biomédica. Los centros debemos garantizar la privacidad de los participantes del estudio, ya que estamos gestionando la información más sensible de las personas. Los investigadores requieren asesoramiento continuo y experto para gestionar las necesidades de sus proyectos en términos de protección de datos personales.

En ISGlobal entendemos la protección de datos personales como un elemento central de reputación y cumplimiento que importa para toda la institución.

Nuestro objetivo final es crear una cultura institucional hacia la protección de datos personales. Esto se consigue principalmente gracias a:

1) un enfoque integral de los POPD, que vaya más allá de la regulación,

Nuestro enfoque va más allá de la regulación y concibe los POPD íntimamente vinculados a las implicaciones éticas y de ciencia abierta de los proyectos. Por lo tanto, se analiza desde esta perspectiva más amplia y no como una cuestión aislada.

2) la implicación de diferentes perfiles y áreas en la institución,

Para ello, en 2017 establecimos un grupo de trabajo interno compuesto por el Gerente de Investigación, quien fue designado como Delegado de Protección de Datos en 2018, el Gerente Jurídico, el Gerente de TI y miembros representantes de las áreas de RRHH, Comunicación, Estadísticas, Capacitación y Compras. . Este grupo de trabajo junto con el apoyo de asesores externos es el responsable de la implementación del GDPR y de la ley española de protección de datos personales y del seguimiento de nuestra política interna en materia de POPD.

3) un sistema de informes que incluya a los Comités Directivo y Científico, al Comité de Cumplimiento y a la Administración,

Los miembros del grupo de trabajo mencionado anteriormente participan en varios órganos de gobierno de la institución, vinculando los requisitos del POPD con las políticas y procedimientos institucionales, científicos, de cumplimiento y de administración.

4) la implementación de varias actividades y acciones,

Destacando: i) un apoyo continuo a los investigadores y sus equipos en cualquier materia relacionada con POPD, ii) actividades continuas de formación y debate, tanto seminarios generales como cursos específicos que respondan a las características de los proyectos, iii) la implementación de evaluaciones y auditorías externas, que identifican nuevas áreas de mejora, y iv) la elaboración de material específico (folletos y vídeos), y herramientas para facilitar la gestión de POPD (sistema de notificación de incidencias, plantillas - DPIA, formulario de consentimiento informado, protocolos, etc.).