MINISTERIO
DE EMPLEO
Y SEGURIDAD SOCIAL

SECRETARÍA DE ESTADO
DE LA SEGURIDAD SOCIAL

# PROPUESTA DE LA GERENCIA DE INFORMÁTICA DE LA SEGURIDAD SOCIAL PARA LA ADECUACIÓN AL RGPD DESDE EL ROL DE ENCARGADO DEL TRATAMIENTO

---

Proyecto de adecuación

**Dirección de Seguridad, Innovación y Proyectos**

2017 / 12 / 07

Gerencia de Informática
de la Seguridad Social

# INDICE

# 1. INTRODUCCIÓN

El objeto del presente documento es dar a conocer el proyecto desarrollado por la Gerencia Informática de la Seguridad Social para proponer un modelo de trabajo que permita a la Seguridad Social dar cumplimiento al nuevo Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (RGPD), en el ámbito de una organización grande y compleja como la Secretaría de Estado de la Seguridad Social.

Este modelo de trabajo propuesto se basa en la experiencia que hay actualmente en la gestión de la seguridad de los sistemas de información, la adecuación de los mismos a la normativa de protección de datos (LOPD) y al Esquema Nacional de Seguridad (ENS), así como una larga experiencia en aplicar medidas de seguridad en Tecnologías de la Información y Comunicaciones (TIC).

El objeto del proyecto: Adecuación al RGPD en la Seguridad Social, ha consistido en la definición y desarrollo de los requisitos y controles que demanda la nueva normativa, principalmente en los aspectos relacionados con la aplicación de las medidas técnicas y organizativas necesarias para dar cumplimiento al nuevo Reglamento, garantizando con ello la salvaguarda de los derechos de los afectados, en especial de los ciudadanos, principal colectivo afectado en el tratamiento de los datos de carácter personal que se gestionan en la organización, y la minimización en el tratamiento de los datos que les puedan afectar.

La Gerencia Informática de la Seguridad Social, órgano con personalidad jurídica y plena capacidad de obrar, que actúa como Servicio Común para la gestión y administración de las tecnologías de la información y las comunicaciones en el sistema de Seguridad Social, ha asumido la definición, coordinación y gestión de la ejecución de este proyecto en su calidad de encargado de tratamiento en relación a los distintos Órganos Directivos adscritos a la Secretaría de Estado.

## 1.1. CONTENIDO DEL DOCUMENTO

Este documento se desarrolla en los apartados siguientes:

- El enunciado de la situación actual, incluyendo las responsabilidades de la GISS.
- Una referencia al inventario de tratamientos con datos personales en la Seguridad Social.
- El buen cumplimiento del ENS y el valor de esta situación en lo que se refiere a medidas de seguridad de los sistemas y su aplicación al RGPD
- Las buenas prácticas de GISS en la gestión de la seguridad de los sistemas, mediante las revisiones de seguridad, etc.
- El desarrollo de los aspectos más relevantes tenidos en cuenta para este proyecto, con los siguientes apartados:
    - Los factores de éxito
    - Los requisitos necesarios más importantes a tener en cuenta.
    - La figura del Delegado de Protección de Datos.
    - Análisis de la situación inicial a partir del caso de uso de la GISS como responsable del tratamiento y encargado, generalización al resto de la organización de la Seguridad Social impactada por el RGPD en base a los ficheros LOPD existentes.
    - Definición de un plan de proyectos a desarrollar para sistematizar de forma homogénea y común en toda la organización de Seguridad Social la adecuación al RGPD.
    - El modelo unificado de controles como instrumento para hacer seguimiento del grado de adecuación.
    - La identificación de trabajos prioritarios mediante los requisitos y controles (canal de atención a los interesados).
    - Los resultados obtenidos.
    - Colaboración con el CCN para la valoración de la herramienta PILAR.

## 2. EL CONTEXTO

La Gerencia Informática de la Seguridad Social (en adelante GISS) presta actualmente un servicio común y actúa en lo relativo a los datos de carácter personal actúa como encargada de tratamiento a las Entidades Gestoras, Servicios Comunes y demás Unidades dependientes de la Secretaría de Estado de la Seguridad Social:

- Tesorería General de la Seguridad Social (TGSS).
- Instituto Nacional de la Seguridad Social (INSS).
- Instituto Social de la Marina (ISM).
- Intervención General de la Seguridad Social (IGSS).
- Dirección General de Ordenación de la Seguridad Social (DGOSS).
- Servicio Jurídico de la Administración de la Seguridad Social (SJASS).


*Figura 1: La GISS como encargada de tratamiento de la Seguridad Social*

Este servicio está amparado por el Real Decreto 703/2017, de 7 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Empleo y Seguridad Social. En la Disposición Adicional Segunda atribuye competencias a la GISS como encargada de tratamiento informático. En concreto, las siguientes:

- La elaboración y proposición a las Entidades Gestoras, Tesorería General de la Seguridad Social e Intervención General de la Seguridad Social de los planes directivos de sistemas de tecnologías de la información y de las telecomunicaciones, para su posterior presentación ante el Consejo general de tecnologías de la información y las comunicaciones de la Seguridad Social.
- La propuesta de creación, desarrollo y modificación de los sistemas de información.
- La evaluación, auditoría e inventario de los sistemas de información vigentes y la propuesta de modificaciones a estos, a fin de garantizar su perfecta coordinación en el esquema general de actuación.
- La creación, custodia y administración de las bases de datos corporativas del sistema, así como los sistemas de seguridad y de confidencialidad.
- El mantenimiento y actualización de los medios telemáticos utilizados para la transmisión de información, así como los correspondientes sistemas informáticos.

Además, el Informe Jurídico 0333/2012 emitido por la Agencia Española de Protección de Datos (AEPD), delimitó la posición de la GISS como encargada de tratamiento en relación a los servicios informáticos que prestaba a las Entidades Gestoras y Servicios Comunes de la Seguridad Social, siempre que sobre los mismos no decidiera sobre la finalidad, uso o tratamiento de los datos que se manejan en estos organismos y que contienen datos de carácter personal.

## 2.1. EL INVENTARIO ACTUAL DE TRATAMIENTOS LOPD

La Seguridad Social cuenta actualmente con alrededor de 1.800 ficheros con datos de carácter personal declarados en el Registro General de Protección de Datos. Esto es fruto de una gran demanda de tratamientos en los Servicios Centrales y, sobre todo, en las Direcciones Provinciales, para atender los servicios que la Seguridad Social presta en todo el país. Un resumen de este inventario por Unidades de gestión de la Secretaria de Estado de la Seguridad Social, se muestra a continuación en la "*Tabla1. Número de tratamientos LOPD declarados en la Seguridad Social".*

Este número tan alto deriva en una necesidad de control por parte de las direcciones de las Entidades Gestoras y Servicios Comunes.

| Entidad Gestora o Servicio Común de la Seguridad Social | Servicios centrales | Direcciones provinciales | Total |
|---|---|---|---|
| Tesorería General de la Seguridad Social (TGSS) | 21 | 349 | **370** |
| Instituto Nacional de la Seguridad Social (INSS) | 30 | 1.256 | **1.286** |
| Instituto Social de la Marina (ISM) | 19 | 29 | **48** |
| Intervención General de la Seguridad Social (IGSS) | 6 | | **6** |
| Dirección General de Ordenación de la Seguridad Social (DGOSS) | 13 | | **13** |
| Servicio Jurídico de la Administración de la Seguridad Social (SJASS). | 2 | | **2** |
| Gerencia Informática de la Seguridad Social (GISS) | 10 | | **10** |
| Secretaría de Estado de la Seguridad Social (SESS) | 13 | | **13** |
| | **114** | **1.634** | **1.748** |

*Tabla 1: Número de tratamientos LOPD declarados en la Seguridad Social.*

A lo largo de los últimos años esta complejidad se ha abordado buscando una "economía de escala"; es decir, medidas comunes que beneficien a la mayor cantidad de tratamientos mediante una estrategia de seguridad común. La implantación de cumplimiento de la legislación de protección de datos y del Esquema Nacional de Seguridad ha sido realizada mediante auditorías periódicas y planes de adecuación comunes a toda la organización.

## 2.2. LA ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD (ENS)

La Seguridad Social, que cumple con la normativa del ENS, tiene declarados un número similar de sistemas de información bajo el Esquema Nacional de Seguridad (ENS).

Los sistemas de información declarados en el ENS no tienen por qué coincidir con los tratamientos LOPD por varios motivos:

- Hay sistemas de información que no tratan datos personales y, como es evidente, no tienen que estar registrados como tratamientos LOPD.
- Un tratamiento LOPD puede reunir varios sistemas de información o viceversa.

Sin embargo, en números redondos, existe un número similar de sistemas bajo el ENS que de tratamientos LOPD, considerando los sistemas y tratamientos declarados en los Servicios Centrales.

En la siguiente tabla se muestra el número de sistemas declarados en el ENS y el número de ellos que contienen ficheros/tratamientos de datos personales, ver detalle en la "*Tabla 2: Número de sistemas de información definidos bajo el ENS en la Seguridad Social. Se distinguen los que tratan datos personales".*

| Entidad Gestora o Servicio Común de la Seguridad Social | Nº total sistemas | Nº sistemas con datos personales |
|---|---|---|
| Tesorería General de la Seguridad Social (TGSS) | 62 | 55 |
| Instituto Nacional de la Seguridad Social (INSS) | 21 | 21 |
| Instituto Social de la Marina (ISM) | 36 | 36 |
| Intervención General de la Seguridad Social (IGSS) | 13 | 1 |
| Dirección General de Ordenación de la Seguridad Social (DGOSS) | 15 | 5 |
| Servicio Jurídico de la Administración de la Seguridad Social (SJASS). | 2 | 2 |
| Gerencia Informática de la Seguridad Social (GISS) | 11 | 8 |
| Secretaría de Estado de la Seguridad Social (SESS) | 0 | 0 |
| Total | **160** | **128** |

*Tabla 2: Número de sistemas de información definidos bajo el ENS en la Seguridad Social. Se distinguen los que tratan datos personales.*

## 2.3. REVISIONES DE SEGURIDAD

La Seguridad Social ha llevado a cabo de manera periódica planes para la adaptación e implantación progresiva los controles y requisitos exigidos por varias normas de seguridad, que incluyen no solo la legislación de protección de datos personales, sino también por otras regulaciones sobre la seguridad (ENS, eIDAS[1], etc.).

Dentro de esos planes bajo control y supervisión de la GISS se han llevado a cabo principalmente tres tipos de revisiones de seguridad:

- Auditorías de cumplimiento (ENS y LOPD).
- Análisis de riesgos.
- Test de intrusión. Pruebas de carácter técnico con el objetivo de encontrar puntos débiles en la infraestructura informática.

A continuación, se detallan las revisiones periódicas de seguridad impulsadas desde la GISS y que se han plasmado en actuaciones de diversa índole en la organización durante los últimos cinco años, como puede verse en la "*Tabla 3: Revisiones de seguridad impulsadas en los 5 últimos años en la Seguridad Social".*

[1] *La GISS es prestador de servicios de confianza denominada ACGISS y emite certificados electrónicos cualificados de empleado público y de Organismo, conforme con el Reglamento eIDAS. Por ello ha pasado en 2017 una auditoria de cumplimiento.*

| Tipo de revisión de seguridad | Año finalización | Alcance de la revisión |
|---|---|---|
| Audioría LOPD | 2013 | Toda la Seguridad Social |
| | 2015 | Toda la Seguridad Social |
| | 2017 | Toda la Seguridad Social |
| Auditoría ENS | 2016 | Toda la Seguridad Social |
| Análisis de riesgos | 2014 | Toda la Seguridad Social |
| | 2016 | Toda la Seguridad Social |
| Test de intrusión | 2015 | Sistemas informáticos centrales |
| | 2016 | Sistemas informáticos centrales |
| | 2017 | Sistemas informáticos centrales |

*Tabla 3: Revisiones de seguridad impulsadas en los 5 últimos años en la Seguridad Social.*

Estas revisiones de seguridad han permitido establecer un ciclo de mejora continua en la gestión de la seguridad, formado por una fase inicial de revisión y otras posteriores de adecuación. También han servido para concienciar a todos las unidades de la Secretaría de Estado de la importancia de la seguridad de la información.

# 3. EL PROYECTO DE ADECUACIÓN AL RGPD

Visto el contexto anterior, tras la entrada en vigor del nuevo Reglamento Europeo de Protección de Datos, la GISS inició una serie de acciones encaminadas a la implantación progresiva de la nueva normativa en la organización. Se realizaron sesiones informativas sobre el nuevo Reglamento y su impacto en mayo de 2016, impartidas por la AEPD a personal directivo de la Seguridad Social. GISS realizó sesiones de divulgación al Comité de Seguridad, en Jornadas de Directores Provinciales, etc.

Este proyecto *"Adecuación al RGPD en la Seguridad Social"* se inició en el primer semestre de 2017 en el seno de la GISS, para obtener su objetivo de implantar requisitos y sus controles que demanda el RGPD, se determinó analizar que trabajos debería realizar la GISS para adecuar los ficheros de los cuales es responsable y también aquellos encaminados a cumplir su rol de "Encargado de Tratamiento" según el RGPD. Con ello se determinó en base a los requisitos que se establecieron y que se ciñen a una interpretación del articulado del RGPD, cuál era la situación de cumplimiento del RGPD tanto en su rol de *"responsable de tratamiento"* como de *"encargado de tratamiento"*. Esto permitió determinar el "gap" existente entre la situación en ese momento y la que debería tenerse a partir del 25 de mayo de 2018 para dar cumplimiento al RGPD. Y definir cuáles serían las acciones a realizar y las potenciales implicaciones en los diferentes responsables que establece el RGPD: "Delegado de Protección de Datos - DPD", "Responsable del Tratamiento - RT", "Encargado del Tratamiento - ET", "autoridad de control y supervisión - AEPD", "Interesado", etc.

En el marco del proyecto y como resultado del mismo se ha propuesto un plan de proyectos a realizar de carácter organizativo, normativo y técnico e identificando responsables. Esta modelización de los trabajos podrá ayudar a llevar a cabo la adecuación al RGPD en la Organización de la Seguridad Social, que por su misión lleva a cabo tratamientos intensivos y extensos de datos de carácter personal.

Los resultados del mismo fueron presentados al Delegado de Protección de Datos que recae en la dirección del Servicios Jurídico de la Seguridad Social (SJASS) y que fue nombrado por el Secretario de Estado en febrero de 2017 a propuesta del Gerente de Informática y derivado de la inquietud manifestada por la Gerencia sobre la necesidad de nombrar esta figura para que la misma pudiera liderar e impulsar en las Unidades de Gestión, responsables del tratamiento, la convergencia al RGPD y conseguir con ello una adecuación basada en políticas, normas, procedimientos, herramientas comunes y la adecuación técnica de los sistemas de información, contando para ello con el apoyo de la Gerencia como encargado del tratamiento y catalizador común de la seguridad TIC.

A continuación se describen los aspectos más relevantes tenidos en cuenta en el proyecto y los resultados obtenidos por el mismo.

Se determinó que existían una serie de factores que hacían que el nuevo proyecto de adecuación al RGPD tuviera unas dificultades inherentes que no se habían dado antes, y que hizo ver a la GISS la necesidad de un análisis especial de los factores de riesgo del proyecto o, dicho en sentido positivo, los factores de éxito.

Veámoslos a continuación.

## 3.1. FACTORES DE ÉXITO DEL PROYECTO

Los riesgos inherentes a la adecuación al RGPD en la Seguridad Social fueron los siguientes:

- Indeterminación de los requisitos de seguridad. El RGPD deja abiertos algunos puntos de interpretación, lo cual es lógico dado que es una norma europea, pero la concreción de esos puntos no estaban cerrados aún por la nueva Ley de protección de datos, que estaba en fase de desarrollo.
- Cambio a la seguridad activa. Mientras que la LOPD es determinista (clasifica concretamente los tipos de datos y las medidas de seguridad sin dar margen a la adaptación a cada organización) y reactiva (no se adelanta a los problemas) el RGPD está orientado al análisis de riesgos y a la toma previa de medidas antes de que se materialicen los problemas.
- Reubicación de ciertos perfiles del ENS. El ENS recoge las figuras del responsable de seguridad y el comité de seguridad, que no están recogidas en el RGPD. Estas figuras deben existir por el mero hecho de cumplir con el ENS y ahora deben coordinarse con la nueva figura que aporta el RGPD: el Delegado de Protección de Datos (en adelante DPD).

Estos riesgos del proyecto pueden ser vistos como factores de éxito si se tienen en cuenta las medidas mitigadoras. En este proyecto se han considerado las siguientes que se describen en la *Tabla 4: Riesgos relevantes del Proyecto y factores de éxito.*

| Riesgo del proyecto | Factores de éxito |
|---|---|
| Indeterminación de los requisitos de seguridad. | Utilización del ENS como marco técnico de medidas de seguridad. El ENS proporciona un complemento muy importante en aspectos tecnológicos. |
| Cambio a la seguridad activa | Realización de un análisis de riesgos general para concretar las medidas a cubrir.<br>Complementarlo con evaluaciones de impacto en la privacidad sólo en los casos de especial riesgo en la privacidad.<br>Implantación de procedimientos de trabajo que sirvan para la aplicación práctica y concreta del RGPD, para:<br>• Poder medir y demostrar el trabajo de prevención de los problemas de seguridad.<br>• Ubicar a las unidades de la organización en los trabajos y responsabilidades concretas que se deben desarrollar. |
| Reubicación de ciertos perfiles del ENS | Establecer procedimientos de trabajo que persigan la coordinación entre el DPD, el responsable de seguridad y el comité de seguridad y que se basen en:<br>• Establecer las función del responsable de seguridad como unidad de apoyo al<br>• Establecer la función del comité de seguridad como supervisor de la adecuación RGPD |

*Tabla 4: Riesgos relevantes del Proyecto y factores de éxito.*

Finalmente se ha considerado como una ventaja, que en este caso se presenta como oportunidad muy importante el reaprovechamiento de los avances conjuntos de la LOPD y el ENS, pues en la mayoría de los requisitos de seguridad del RGPD resultan de la unión de estos otros dos (Figura 2. El RGPD reúne los controles ya existentes del ENS, LOPD y su reglamento de desarrollo (RD LOPD) además de otros exclusivos).

.

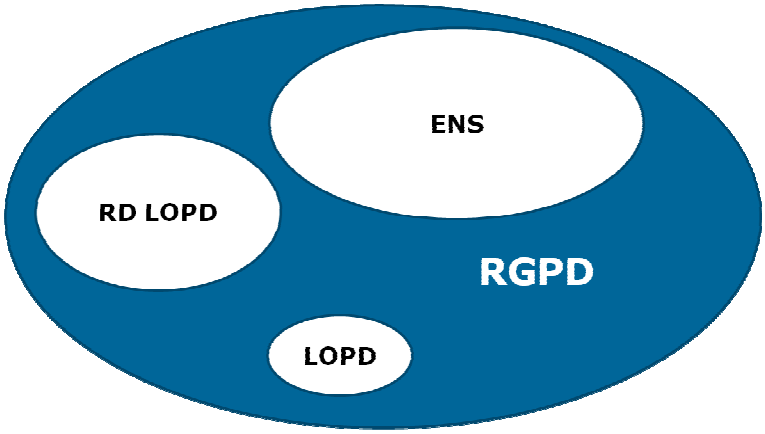


*Figura 2. El RGPD reúne los controles ya existentes del ENS, LOPD y su reglamento de desarrollo (RD LOPD) además de otros exclusivos.*

## 3.2. REQUISITOS GENERALES DEL PROYECTO

Antes del comienzo del proyecto se identificaron una serie de requisitos generales:

- Garantizar la salvaguarda efectiva de los derechos de los afectados. Ello supone tener que definir nuevos procedimientos que den cumplimiento efectivo a estos derechos, sin contar con directrices previas claras que establezcan las acciones a acometer para dar cumplimiento a los mismos. Es necesario definir estos procedimientos estableciendo unos plazos razonables de resolución a estas solicitudes de tal manera que se eviten dilaciones indebidas en la contestación que puedan generar indefensión en los titulares de los datos.
- Establecer mayores medidas de control y supervisión de las prestaciones de servicios llevadas a cabo por terceros o entidades externas en los que resulten afectados directa o indirectamente tratamientos de datos de carácter personal titularidad de la Seguridad Social en cuanto que es necesario garantizar la adecuada capacitación y garantía de este tipo de empresas. Solicitud de medidas de seguridad más exhaustivas con el objeto de que den cumplimiento al principio de responsabilidad activa en el ámbito de sus competencias, etc.
- Garantizar la existencia de unos cauces adecuados de comunicación y notificación con la Autoridad de Control (AEPD, CCN, etc.) para dar respuesta a todos los requerimientos que el RGPD establece a todas las organizaciones: garantizar que cumple con la normativa, notificaciones de violaciones de seguridad, notificaciones de tratamientos con un alto riesgo, etc.
- Que el personal de la organización pueda tener una formación adecuada para conocer sus funciones y competencias en relación a esta nueva norma, garantizando el adecuado tratamiento de estos datos por parte de este colectivo una vez que sea obligatoria la aplicación de la norma, teniendo en cuenta que hay nuevos requerimientos, nuevos Principios, etc.
- Garantizar que tanto en relación a los tratamientos de datos de carácter personal (que calificamos como DPD) ya existentes, como en los nuevos, se apliquen criterios de seguridad por defecto y desde el diseño tanto en los sistemas ya existentes como en los nuevos desarrollos de tratamientos automatizados que se efectúen en la organización.

Para cada uno de los requisitos anteriores, se han definido una serie de medidas de mitigación, que se describen a continuación en la *Tabla 5: Requisitos y medidas de implementación.*

| Requisito | Medidas de implementación |
|---|---|
| La salvaguarda efectiva de los derechos de los afectados, tras el reconocimiento de nuevas modalidades de derechos, | Se han definido los procedimientos y cauces de trabajo internos para dar respuesta efectiva a estos nuevos derechos<br>Definir las herramientas a utilizar para el ejercicio de estos nuevos derechos.<br>Se han previsto las unidades que deben intervenir para la resolución efectiva de los mismos.<br>.<br>Se han definido plazos de tiempo en la organización, en la medida de lo posible ajustados para la resolución efectiva a este tipo de solicitudes , tratando de dar solución a la indefinición de plazos existente con la nueva normativa, |
| Riesgos derivados de tratamientos externalizados | Elabora nuevas cláusulas a incluir en los contratos de prestación de servicios con encargados de tratamiento que contemplen los nuevos requerimientos exigidos por la normativa:<br>- Garantizar la adecuada diligencia y capacitación del encargado para la prestación de los servicios.<br>- Cumplir con las medidas de seguridad, incluidas la obligación de acreditar ante la autoridad competente el cumplimiento de la norma en los apartados que son de su exclusiva competencia. |
| Garantizar la existencia de unos adecuados cauces de comunicación/notificación/colaboración requeridos por la nueva norma ante la Autoridad de Control (AEPD/CCN) | - Definir las herramientas y cauces de comunicación con la autoridad de control (LUCIA, etc.).<br>- Acotado los diversos formatos para el envío efectivo de la información a la autoridad de control (pdf, etc.). |
| Necesidad de nuevos conocimientos en protección de datos por parte del personal de la organización para el cumplimiento efectivo de la nueva norma en relación a los tratamientos de datos personales existentes en la organización (principio de responsabilidad activa -accountability-, etc.). | - Definir la impartición de cursos de formación en esta materia para todo el personal de la organización, centrados en las tareas que debe acometer este colectivo para el adecuado tratamiento de estos datos.<br>- Definir acciones específicas para formar también a los responsables internos de cada uno de los tratamientos con datos personales identificados en la organización. |
| Garantizar de manera efectiva el cumplimiento de la seguridad por defecto y desde el diseño. | - Definir por cada tratamiento identificado plazos de conservación de la información.<br>- En los nuevos desarrollos de sistemas que tratan con datos de carácter personal, identificar la posibilidad de aplicación de criterios comunes de seudonimización, en aquellos tratamientos que los precisen.<br>- En los desarrollos de los sistemas definir y aplicar metodologías de desarrollo seguro.<br>- Estudiar las necesidades de cada tratamiento para adecuar |

| | |
|---|---|
| | el control de los accesos a lo requerido en cada uno. |

*Tabla 5: Requisitos y medidas de implementación*

## 3.3. NOMBRAMIENTO DE UN DELEGADO DE PROTECCIÓN DE DATOS

Dado que el nuevo RGPD establece como una de las novedades fundamentales el nombramiento del Delegado de Protección de Datos como figura a través de la cual centralizar la supervisión y coordinación de la implantación y cumplimiento de esta normativa, se procedió en la Seguridad Social al nombramiento de esta figura.

Así, el Delegado de Protección de Datos en la Seguridad Social fue designado atendiendo a sus cualidades profesionales. En concreto, fue la Dirección del Servicio Jurídico de la Administración de la Seguridad Social, órgano con conocimientos especializados en derecho y con experiencia y conocimientos en torno a los principios en los que se basa la regulación de los tratamientos de datos de carácter personal así como la adecuada protección de los derechos de los afectados.

Este órgano está siendo apoyado en la labor de implantación de las medidas técnicas y organizativas por la GISS.

De esta manera, a través de este nombramiento se han cubierto en relación a la organización, las dos partes que reclamaba el nuevo RGPD, el perfil jurídico especializado en la normativa vigente de protección de datos, y, el perfil técnico, al mantenerse la figura del Responsable de Seguridad de la organización en la GISS, recayendo está en la Dirección de Seguridad, Innovación y Proyectos (DSIP), que si bien, no se reconoce expresamente en la nueva normativa, su existencia se ha considerado absolutamente necesaria para apoyar, realizar y asesorar en la coordinación de la implantación de las medidas técnicas y organizativas exigidas, contando este órgano con una amplia experiencia en labores de implantación dentro de este ámbito.

## 3.4. ANÁLISIS INICIAL DE CUMPLIMIENTO RGPD EN LA GISS

La GISS durante el primer semestre del año 2017 coordinó e impulsó un plan para el análisis del estado de cumplimiento con el RGPD dentro de su ámbito, como responsable y encargado del tratamientos de datos de carácter personal (sistema de confidencialidad denominado SILCON, etc.), excluyendo de este análisis el resto de tratamientos de Entidades Gestoras, Servicios Comunes y demás Unidades de la Secretaria de Estado de la Seguridad Social) y elaboró una propuesta de proyectos de seguridad que deberían llevarse a cabo estableciendo una metodología común para la Seguridad Social para abordar la adecuación.

Las tareas de este análisis fueron, resumidamente, las siguientes:

- Identificar con carácter general el impacto del RGPD.
- Evaluar la situación existente y grado de implantación de los controles y requisitos de esta normativa en las distintas áreas responsables de GISS, identificando el grado actual de cumplimiento de cada uno de estos controles.
- Identificar y valorar por cada requisito las variables a tener en cuenta y a través de las cuales acotar la importancia de cumplir individualmente con cada requisito identificado en el nuevo Reglamento.
- Definir un Plan de Proyectos a abordar para garantizar la progresiva adaptación a esta normativa, delimitando las distintas Áreas responsables intervinientes en cada caso en esta implantación.
- Establecer una planificación para abordar cada uno de los Proyectos identificados.

De los puntos indicados, los principales resultados obtenidos por la GISS a través de este plan, y en virtud de los cuales se ha basado y diseñado el actual modelo de implantación del nuevo RGPD en todo el ámbito de la Secretaria de Estado de la Seguridad Social, han sido:

- Medida del grado de cumplimiento de los artículos del RGPD.
- Identificación de los mayores riesgos de seguridad. En concreto, para la identificación de estos riesgos se han tenido en cuenta:

  - La probabilidad de ocurrencia de un hecho negativo asociado a la falta de cumplimiento de un requisito.
  - Impacto desde diversos puntos de vista:
    - Impacto económico: Daño económico que se sufre por la ocurrencia de un hecho negativo asociado a la falta de cumplimiento de un requisito.
    - Impacto reputacional: Daño a la imagen y reputación que se sufre por la ocurrencia de un hecho negativo asociado a la falta de cumplimiento de un requisito.
    - Impacto "de negocio": Daño a las actividades del servicio prestado por la Seguridad Social (pérdida del servicio en el canal presencial, telemático y telefónico, reducción de los plazos de recuperación del servicio, etc.) que se sufre por la ocurrencia de un hecho negativo asociado a la falta de cumplimiento de un requisito.
- Definición de acciones y planes de implantación relativos a los requisitos actualmente no implantados en la Entidad.

Como consecuencia de la situación identificada en la organización se definió un plan de Proyectos cuyo objetivo es abordar el establecimiento de los controles de seguridad para el cumplimiento, aspecto este en el que se era más deficitario, así como abordar la implantación de los necesarios controles que más directamente pudieran incidir, o garantizar, directa o indirectamente la salvaguarda de los derechos de los afectados.

La relación de proyectos ha sido la siguiente:

- **PR01 Designación del Delegado de Protección de Datos**: Una vez designado se debe proceder a la asignación, de los medios, de recursos normativos y de procedimientos, para el cumplimiento de sus funciones, especialmente en las concernientes al asesoramiento experto en materia de protección de datos de carácter personal.

En concreto, los procesos y acciones se ciñeron a los aspectos de recursos normativos y de procedimiento con el que el DPD debe contar para el desarrollo de su función y que fueron definidos para la implantación de este proyecto. Se pueden ver a continuación en la *Figura 3: Tareas del proyecto del Delegado de Protección de Datos.*

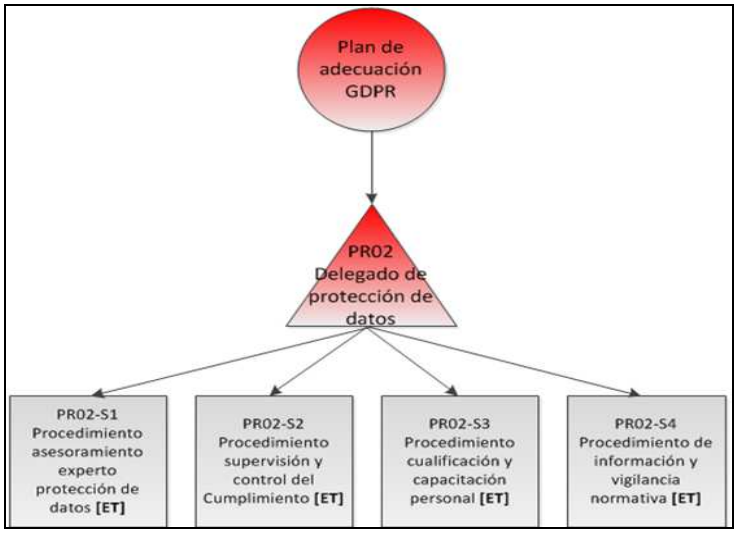


*Figura 3: Tareas del proyecto del Delegado de Protección de Datos.*

Los resultados de este proyecto han sido la elaboración de los siguientes documentos:

- Procedimiento de gestión de normativa de aplicación del RGPD.
- Procedimiento de actualización de la normativa de aplicación.
- Procedimiento de resolución de dudas de interpretación de la normativa.
- Procedimiento para el seguimiento de no conformidades.
- Procedimiento de formación y concienciación.

- Diseño de alto nivel del canal de comunicación del DPD.

- **PR02 Evaluación de impacto:** Implantación de un procedimiento para el análisis, desde el punto de vista de protección de datos, de las operaciones y finalidades del tratamiento, la necesidad y proporcionalidad de las operaciones de tratamiento, los riesgos que corren los derechos y libertades de los titulares de los datos de conformidad con el artículo 35 del GDPR y las medidas previstas para afrontar los riesgos.

En concreto, los procesos y acciones que fueron definidos para la implantación de este proyecto se pueden ver a continuación en la *Figura 4: Tareas del proyecto de Evaluación de Impacto.*

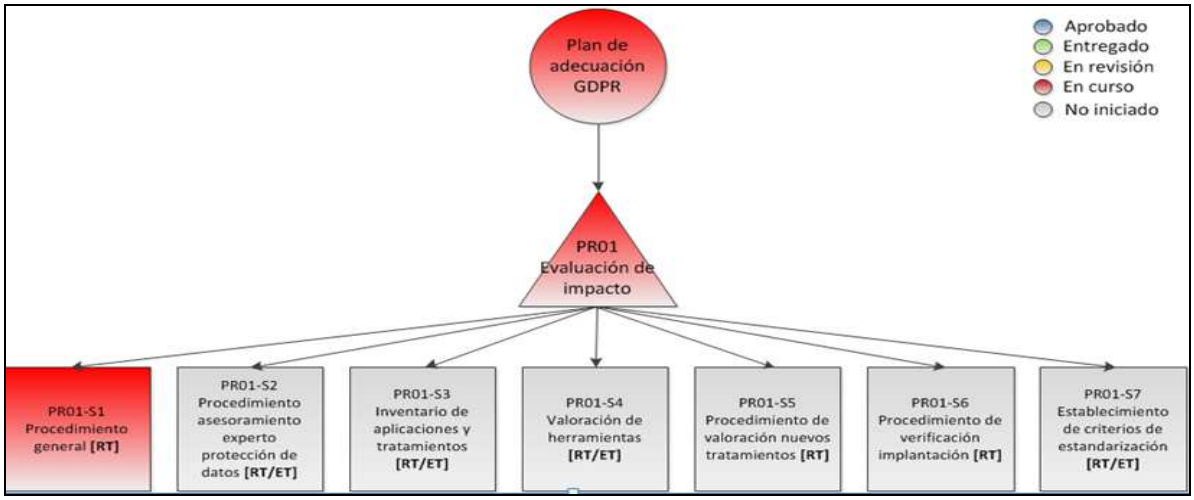


*Figura 4: Tareas del proyecto de Evaluación de Impacto.*

Los resultados de este proyecto han sido los siguientes:

- Definición del riesgo de tratamientos.
- Procedimiento de actualización del registro de tratamientos.
- Política para la realización de EIPDs.
- Procedimiento de revisión y seguimiento de EIPDs.
- Calculador de riesgos para EIPDs.
- Informe de EIPDs.

- **PR03 Adecuación de principios:** Obtención efectiva de consentimiento para el tratamiento de datos personales, cuando el consentimiento es la base jurídica de un tratamiento. Definición, desarrollo e implicaciones del resto de principios reconocidos por el nuevo RGPD, minimización de datos, responsabilidad activa, etc.

En concreto, los procesos y acciones que fueron definidos para la implantación de este proyecto se pueden ver en la siguiente *Figura 5: Tareas del proyecto de Adecuación de Principios.*

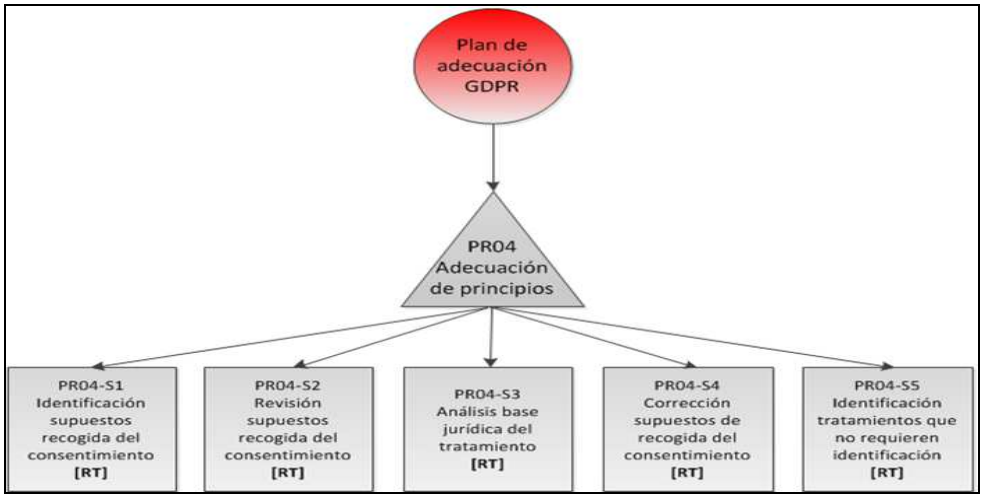


*Figura 5: Tareas del proyecto de Adecuación de Principios*

Los resultados de este proyecto han sido los siguientes:

- Verificación de supuestos de recogida del consentimiento.
- Revisión de supuestos de recogida del consentimiento.
- Análisis de la base jurídica del tratamiento.
- Corrección de los supuestos de recogida del consentimiento.
- Identificación de tratamientos que no requieren identificación.

- **PR04 Transparencia y ejercicio de derechos:** Existencia de un procedimiento general para hacer efectivo el ejercicio de los derechos por parte de los interesados en la forma descrita por el RGPD.

En concreto, los procesos y acciones que fueron definidos para la implantación de este proyecto se pueden ver gráficamente a través de la *Figura 6: Tareas del proyecto de Transparencia y ejercicio de derechos.*

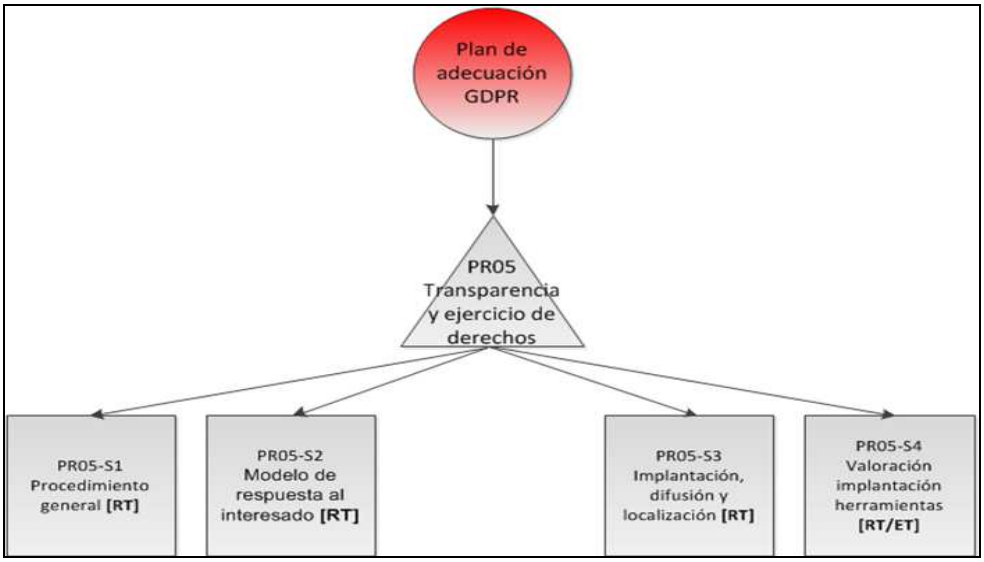


*Figura 6: Tareas del proyecto de Transparencia y ejercicio de derechos.*

Los resultados de este proyecto han sido los siguientes:

- Procedimiento general de atención a los derechos.
- Modelo de respuesta al interesado.

- Un procedimiento para la Implantación, difusión y localización.
- Valoración Implantación herramientas.

- **PR05 Adecuación Obligaciones Generales**: Establecer las bases para el cumplimiento de las obligaciones y requisitos establecidos por el GDPR para el responsable del tratamiento y el encargado del tratamiento.

En concreto, los procesos y acciones previstas para la implantación de este proyecto se pueden ver gráficamente a través de *Figura 7: Tareas del proyecto de Adecuación y obligaciones generales.*

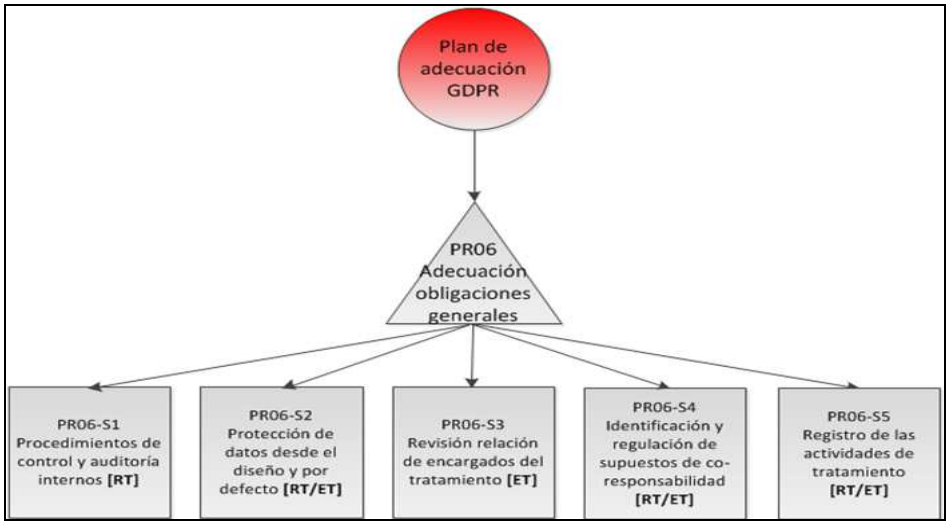


*Figura 7: Tareas del proyecto de Adecuación y obligaciones generales*

Los resultados de este proyecto han sido los siguientes:

- Procedimiento para el cumplimiento de las obligaciones de protección de datos con terceros y modelos tipo asociados.
- Contrato de encargado del tratamiento.
- Inventario y gestión del Registro de tratamientos.

- **PR06 Seguridad de los datos**: Implantación de las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, incluyendo en todo caso las mínimas establecidas por el GDPR.

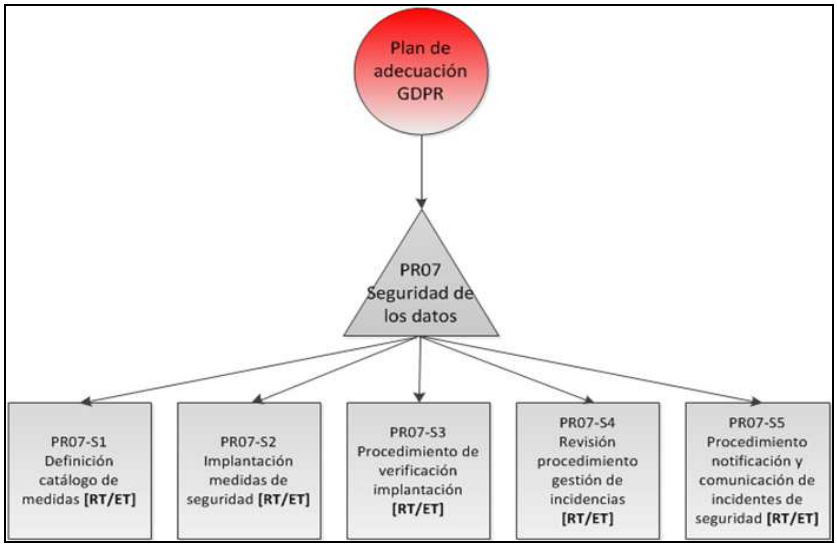


*Figura 8: Tareas del proyecto de Seguridad de los datos.*

Los resultados de este proyecto han sido los siguientes:

- Procedimiento para la realización de auditorías del RGPD y modelo tipo de informe de auditoría.
- Procedimiento de análisis general de riesgos de seguridad.
- Procedimiento de comunicación de brechas de seguridad.
- Diseño funcional de alto nivel del gestor de incidentes.
- Diseño de indicadores y métricas de seguridad.
- Procedimiento de supervisión de la seguridad.

## 3.5. EL MODELO UNIFICADO DE CONTROLES DE SEGURIDAD

El siguiente paso que se acometió fue la búsqueda de una herramienta que permitiera llevar a cabo una gestión e implantación integral de los estándares de seguridad que se están abordando (y de los que el RGPD es uno más)

El Modelo Unificado de Controles de Seguridad (MUC) proviene de la empresa SIA (Sistemas Informáticos Abiertos) y en la GISS se ha desarrollado una implementación “ad hoc” de este modelo mediante una herramienta. Esto ha sido posible porque la GISS tiene un contrato de asistencia técnica, en fase de ejecución con esta empresa, lo que le permite liderar y ejecutar diferentes trabajos de seguridad con este contratista.

El concepto del MUC se centra en el control de seguridad como un conjunto de requisitos que se aplican a la vez en uno o varios estándares de seguridad.

Por ejemplo, que las contraseñas sean robustas es un control que incluye varios requisitos (longitud grande, caracteres especiales, etc.). Este control aplica en varios estándares (RD de desarrollo de la LOPD, ENS, etc.). A su vez pueden haberse recogido “no conformidades” en la última auditoría de seguridad y, sobre la resolución de las no conformidades, se ha hecho un seguimiento. Finalmente sobre los controles se recogen una serie de evidencias que sirven para demostrar cuál es el estado de su seguridad.


*Figura 9: Gráfico conceptual del Modelo Unificado de Controles*

El modelo unificado de controles ha permitido:

- Integrar las distintas normativas de seguridad cuya implantación es objeto de control por la GISS en la organización, estableciendo una interrelación y una conexión entre los distintos controles y requisitos contemplados en cada una de ellas con el objeto de buscar sinergias que permitieran reducir los trámites/trabajos relacionados con la implantación y cumplimiento progresivo de estas normas en la organización. En concreto, las normativas que actualmente han sido incluidas dentro de esta herramienta son: LOPD y su normativa de desarrollo (RDLOPD), Esquema Nacional de Seguridad y el Reglamento eIDAS.
- Así mismo, esta herramienta integra también un gestor documental que ha permitido tener un registro de todas las evidencias relativas al grado de cumplimiento de los controles relativos a estas normativas, seguimiento de No Conformidades, etc.

Lo que esta herramienta ha aportado de cara a facilitar la implantación del nuevo RGPD se resume en

- Identificar los controles o requisitos ya implantados en la organización referentes a la LOPD y su normativa de desarrollo y ENS, que de manera directa o implícita puedan estar contenidos total o parcialmente en los requisitos y controles que demanda el nuevo RGPD, conociendo su estado actual de implantación y cumplimiento en la organización, y facilitando con ello, una gestión centralizada de las tareas a acometer para la implantación gradual de estos controles.
- Identificar los nuevos controles y requisitos que demanda el nuevo RGPD y sobre los cuales ha sido necesario iniciar nuevas acciones de adecuación e implantación, facilitando la gestión integral de su progresiva implantación en las Entidades Gestoras.
- Se ha aprovechado la mayor parte del trabajo realizado de control de cumplimiento e implantación de los controles definidos en estas normativas (LOPD y ENS) y ya acometidos en la organización, para optimizar las labores de implantación de esta nueva normativa, básicamente en la medida en que el nuevo anteproyecto de LOPD, establece que las medidas de seguridad a aplicar para el tratamiento de datos de carácter personal se ha de basar en el Esquema Nacional de Seguridad.
- Ejecución progresiva de todo el ciclo de vida de los controles del RGPD para garantizar su implantación efectiva en la Entidad.
- Obtención periódica de indicadores de revisión de cumplimiento y por tanto de implantación de los controles y requisitos de la norma.
- Registrar evidencia y nivel de cumplimiento y madurez con la frecuencia necesaria para cada control.

Como ya comentamos anteriormente, una buena parte de los controles de seguridad del RGPD que se deben implantar ya han sido analizados por la necesidad de análisis previos de los estándares de seguridad (en medidas tales como el cifrado, registro de actividades de tratamiento, seudoanonimización, seguridad por defecto, etc.).

En términos cuantitativos el reparto de controles es aproximadamente el siguiente:

| | Controles | |
|---|---|---|
| **Estándar** | **Número** | **%** |
| ENS | 116 | **66%** |
| LOPD | 15 | **8%** |
| RDLOPD | 46 | **26%** |
| **RGPD** | 177 | **100%** |

*Tabla 6. Reparto de controles entre los estándares de seguridad.*

## 3.6. CANAL DE ATENCIÓN A LOS DERECHOS DE LOS AFECTADOS

Otra de las prioridades que se identificaron fue la salvaguarda de los derechos de los afectados, en una organización que maneja una cantidad ingente de datos personales de los ciudadanos.

Por ello, se han definido unos criterios de actuación para garantizar que la respuesta a los derechos de los afectados se efectuaba en unos tiempos mínimos de respuesta de acuerdo con los requerimientos de la norma.

Para ello, impulsó una serie de actuaciones destinadas a:

- Definir procesos para dar cumplimiento al ejercicio de los derechos de los afectados (Acceso Rectificación, Supresión, Limitación en el tratamiento, derecho al olvido, portabilidad, etc.) haciendo efectivo el ejercicio de estos derechos en los sistemas de información que pudieran resultar afectados.
- Centralizar en un único sistema la presentación y resolución de solicitudes de ejercicios de derechos. A través de este sistema se pretende que los distintos departamentos y áreas intervinientes en la resolución de este tipo de solicitudes, estén adecuadamente informados y se coordinen las actuaciones para dar respuesta efectiva a los derechos de los mismos.

  Así, una de las opciones que se han fomentado es la de albergar un servicio web en la sede electrónica, con control de acceso para que los ciudadanos puedan ejercer sus derechos.

  En este caso, la solicitud de ejercicio de un derecho por parte de un ciudadano, el servicio envía una alerta (a través de correo electrónico), al titular del tratamiento (Entidad Gestora, Servicio Común y demás unidades dependientes de la Secretaria de Estado de la Seguridad Social) avisándole de la petición, así mismo, llega una notificación de la petición tanto al DPD como a la DSIP (unidad de la GISS) para su conocimiento y la debida coordinación de actuaciones.

  Este servicio contiene además un histórico de las peticiones de derechos ejercidas por los afectados.
- Con respecto a la limitación en el tratamiento de los datos, la solicitud efectiva de este derecho se puede realizar a través de la sede. Además, se han diseñado mecanismos para el bloqueo de los sistemas en los que se acuerde la limitación, estableciendo mecanismos de acceso a los mismos únicamente a los usuarios autorizados y exclusivamente en los casos permitidos por la norma.
- Respecto a los derechos de portabilidad de los datos: La solicitud se puede realizar a través de la sede, una vez debidamente identificado el ciudadano, éste deberá aportar los siguientes datos: Listado de ficheros RGPD que almacenan sus datos, formato en que desea recibir esta documentación (XML o CSV, etc.). Previamente la organización deberá autorizar el ejercicio de este derecho, es decir, deberá revisar que la solicitud esté justificada.

- Con respecto al derecho al olvido: La solicitud se puede realizar a través de sede. En este caso, en la organización ya se han definido, para el caso en que se autoricen el ejercicio de este tipo de solicitudes, procedimientos para la eliminación de la información requerida de manera coordinada para todos los sistemas de la organización que puedan resultar afectados.
- En relación al Derecho de Información:
    1. En un primer momento se ha llevado a cabo una revisión y mejora de las cláusulas informativas ya existentes en la Entidad con el objeto de adecuarse a los contenidos del nuevo RGPD. Estas cláusulas se facilitaron a cada uno de los responsables de tratamiento afectados.
    2. A continuación, se han elaborado modelos de cláusulas informativas que dieran cumplimiento a la norma en relación a nuevos tratamientos identificados o a los tratamientos que no contaban con estos modelos. Así se elaboraron dos tipos de cláusulas informativas que contemplan dos casuísticas, cuando los datos han sido obtenidos por medio del interesado y los casos en que se han obtenido por otros medios.
- En relación al Derecho del Consentimiento:
    1. En un primer momento, se llevó a cabo una revisión y mejora de las cláusulas de solicitud del consentimiento en los casos y en los tratamientos que se identificaron en la organización.
    2. En relación a los nuevos tratamientos LOPD que se identificaron y se detectaron nuevas cláusulas de solicitud del consentimiento.

Por último indicar que, desde la organización, se ha previsto un medio alternativo para el ejercicio de los derechos por parte de los afectados, para el caso de los ciudadanos que no quieran o no puedan realizar este tipo de peticiones a través de la Sede electrónica (https://sede.seg-social.gob.es). En este caso, se ha propuesto una dirección postal a la cual se pueden dirigir todos los afectados. Las peticiones que llegan a través de este medio, se centralizan en el Área responsable y se resuelven siguiendo los procedimientos internos que para el ejercicio de estos derechos, ha previsto la organización.

# 4. RESULTADOS OBTENIDOS

Como resultado del análisis de cumplimiento anterior la GISS inició una serie de acciones encaminadas a la implantación progresiva de la nueva normativa dentro de su organización basándose en las siguientes líneas de actuación:

## 4.1. PROCEDIMIENTOS DE CUMPLIMIENTO RGPD

### 4.1.1. TÉCNICOS

Una vez conocida la situación de su organización, la GISS efectuó un análisis y evaluación de las normativas y procesos que debían ser definidos de manera centralizada para su aplicación uniforme en las distintas Entidades Gestoras con el objeto de dar cumplimiento de manera coordinada a los requerimientos técnicos que actualmente demanda esta normativa.

En base a este análisis, la GISS identificó, definió y elaboró, en su caso, aprovechando buena parte de los procesos que ya tenía definidos para dar cumplimiento a la LOPD, entre otros, las siguientes normativas, procesos, técnicos y organizativos necesarios para garantizar los requerimientos técnicos del RGPD. En concreto:

- Procedimiento de Auditoria.
- Gestión de Incidentes y notificación de violaciones de seguridad.
- Procedimientos para la seudonimización de los datos.
- Seguridad desde el diseño y por defecto.
- Procedimientos para la aplicación de criterios de cifrado de la información en tratamientos con datos personales.

- Procedimiento para la realización de las Evaluaciones de Impacto.
- Registro de las actividades de tratamiento, etc.

### 4.1.2. JURÍDICOS

La GISS ha impulsado la definición de normas y procedimientos para garantizar el cumplimiento de los principios definidos e identificados en el RGPD. Esta documentación sirvió de base para definir acciones concretas para la implantación en las distintas Entidades, prestando atención a la salvaguarda de los derechos de los afectados, tanto ciudadanos como en su caso personal de la organización.

En relación a este ámbito, la GISS impulsó la elaboración entre otras normativas de seguridad:

- Procedimiento que regula el adecuado ejercicio de los derechos de los afectados, en concreto, se han de contemplar los siguientes derechos:

  - Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición)
  - Derecho al olvido
  - Derecho de portabilidad
  - Derecho a la limitación en el tratamiento.

  Estableciendo dentro de estos procedimientos y por cada derecho, los medios, formatos y recursos necesarios para poder hacer efectivos los mismos.

- Normas que garanticen y coordinen el adecuado cumplimiento del principio de Calidad de Datos en la organización. Estas políticas incluyen a su vez, el establecimiento de criterios para la minimización en el tratamiento de datos de carácter personal en la Entidad, la definición de plazos de conservación de los distintos tratamientos, el establecimiento de criterios para el adecuado expurgo y cancelación periódica de la información, etc.

- Normas para garantizar la adecuada transparencia en el tratamiento de datos de carácter personal de la organización (Derecho de Información).

- Normas que garanticen la licitud en el tratamiento de los datos (Derecho del consentimiento), etc.

## 4.2. REVISIÓN Y ACTUALIZACIÓN DE TRATAMIENTOS LOPD YA DEFINIDOS Y REGISTRO DE ACTIVIDADES DE TRATAMIENTO

La siguiente acción que se impulsó desde la GISS con el objeto de acotar el alcance de las medidas técnicas y organizativas que por sus competencias debía coordinar y supervisar de manera centralizada en la organización, es la identificación del número total de tratamientos y de sistemas de información existentes tanto en la GISS como en las distintas Entidades Gestoras a través de los cuales se efectúan tratamientos con datos de carácter personal.

Para ello, se aprovechó todo el trabajo ya realizado en materia de protección de datos personales en la organización, se partió del Registro centralizado de tratamiento de datos de carácter personal existente a través de la herramienta SIGLA (herramienta del Ministerio de Empleo y Seguridad Social –MEYSS), donde estaban identificados todos los ficheros de la Seguridad Social declarados a la AEPD y a continuación, la GISS procedió con los distintos responsables a confirmar la existencia de dichos tratamientos, así como, en su caso, a su actualización y a la identificación de posibles nuevos tratamientos.

De manera paralela, y a través de los registros ya existentes así como de las entrevistas efectuadas con los distintos responsables, se identificaron también todos los sistemas de Información que dan soporte a estos tratamientos.

Tanto los tratamientos identificados como los Sistemas de Información a través de los cuales se gestionan los mismos, fueron adecuadamente registrados con el objeto de dar cumplimiento al registro de actividades de tratamiento exigidos por la nueva normativa en su artículo 30. Este registro se completó con la información que sobre las actividades de cada tratamiento la organización tenía ya recogida en los Documentos de Seguridad LOPD de cada fichero, donde se detallaban las medidas de seguridad que se aplicaban por cada tratamiento, etc.

Tras la aprobación del nuevo RGPD, la GISS identificó que el registro de actividades de tratamiento que se manejaba en la organización no incluía todos los contenidos necesarios para dar cumplimiento al nuevo RGPD, donde en virtud del nuevo principio de Accountability o responsabilidad activa, se deben registrar los aspectos de los tratamientos cuyo cumplimiento corresponde a la organización y que esta debe demostrar en caso de posible reclamación de la AEPD a la organización en cuanto a responsable de tratamiento. Así, finalmente se han incluido en estos registros, las evaluaciones de Impacto, Análisis de Riesgos, revisiones periódicas de los registros de accesos para el caso de tratamientos especialmente sensibles, etc.

Una vez que la organización ha identificado todas las actividades que deben ser objeto de registro en relación a cada uno de los tratamientos con datos de carácter personal que maneja, ha elaborado también estos registros con similares características por cada nuevo tratamiento que se ha identificado en la organización.

Por último, desde la GISS se han definido procedimientos de revisión periódica de estos registros con el objeto de que los mismos permanezcan permanente actualizados, identificando las departamentos o áreas responsables que deben participar en la actualización de éstos.

## 4.3. LA EVALUACIÓN DE IMPACTO COMO MEDIO DE DECISIÓN DE MEDIDAS EN CASO DE RIESGOS ALTOS EN PRIVACIDAD

Otra de las premisas que el nuevo RGPD estableció para la implantación adecuada de las medidas técnicas en los tratamientos con datos de carácter personal fue la realización de una Evaluación de Impacto sobre los mismos.

La GISS ha desarrollado una guía y una herramienta, que complementa el análisis de riesgos de seguridad, y que está basada en la “Guía para una Evaluación de Impacto en la Protección de Datos Personales” publicada por la Agencia Española de Protección de Datos. Se describe a continuación y está soportado por una sencilla herramienta de cálculo de los objetivos anteriores.

A través de la realización de estas evaluaciones, se buscaron los siguientes objetivos:

- Identificar los requerimientos previos tanto técnicos como jurídicos que cada tratamiento por su naturaleza y características demandaba para dar cumplimiento a la normativa.
- Identificar las amenazas relacionadas con el impacto en la privacidad con una cuantificación de los riesgos.
- Plantear un conjunto de medidas de mitigación de los riesgos asociados, priorizarlas y sugerir el grado de implantación de esas medidas.

Sobre un tratamiento en particular consiste resumidamente en los siguientes pasos:

- Determinación del tipo de tratamiento en el que se encuadra el tratamiento particular.
- Determinación de los factores de riesgo.
- Determinación de los riesgos de impacto en la privacidad.
- Revisión de las circunstancias específicas del tratamiento particular.
- Modulación de los riesgos en función de esas circunstancias particulares.
- Priorización de las medidas a tomar en función de la efectividad con que combaten los riesgos.
- Determinación del grado de implantación de cada medida.

### 4.3.1. ENTORNOS DE TRATAMIENTO DE DATOS

En una organización en la que los tratamientos se enmarcan en distintos entornos y cada uno de ellos tiene un perfil predeterminado de factores de riesgo, se ha determinado relevante establecer entornos de tratamientos genéricos que ayuden a realizar evaluaciones de impacto en la privacidad de forma más sistemática en base a criterios comunes que puedan tener los tratamientos objeto de esta evaluación.

En el caso de la Seguridad Social, se han identificado son los relacionados en la *Tabla 7. Factores de riesgo en función de los tipos de tratamiento de datos.*

| | Factores de Riesgo | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Entornos de tratamiento** | Analítica de datos interna (biga data) | Tratamientos masivos | Tratamientos con datos especialmente protegidos. | Analítica de datos (para terceros) | Tecnologías invasivas | Cesiones / Transferencias internacionales de datos | Tratamientos con nuevas categorías de datos / Determinación de perfiles | Tratamientos con datos de menores |
| Entorno de riesgo máximo | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% |
| Entorno central | 0% | 100% | 25% | 0% | 0% | 0% | 0% | 25% |
| Big data (tratamiento interno) | 100% | 100% | 25% | 0% | 0% | 0% | 50% | 25% |
| Big data (tratamiento externo) | 100% | 50% | 25% | 0% | 0% | 100% | 0% | 25% |
| Transferencias nacionales | 0% | 50% | 25% | 0% | 0% | 100% | 25% | 25% |
| Transferencias internacionales | 0% | 50% | 25% | 0% | 0% | 100% | 25% | 25% |
| Transferencias de datos especialmente protegidos de menores | 0% | 50% | 100% | 0% | 0% | 100% | 25% | 100% |
| Resto de tratamientos | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% |

*Tabla 7. Factores de riesgo en función de los tipos de tratamiento de datos.*

### 4.3.2. FACTORES DE RIESGO

En el análisis de seguridad realizado se han considerado las siguientes circunstancias que definen los riesgos de seguridad de una manera general:

- **Analítica de datos interna (big data).** Cuando se traten grandes volúmenes de datos personales a través de tecnologías como la de datos masivos (Big data), internet de las cosas (Internet of Tingas) o el desarrollo y la construcción de ciudades inteligentes (smart cities).
- **Tratamientos masivos.** Cuando el tratamiento afecte a un número elevado de personas o, alternativa o adicionalmente, se produzca la acumulación de gran cantidad de datos respecto de los interesados.
- **Tratamientos con datos especialmente protegidos.** Cuando la recogida tenga como finalidad el tratamiento sistemático y masivo de datos especialmente protegidos.
- **Analítica de datos (para terceros).** Cuando se vayan a utilizar datos personales no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica.
- **Tecnologías invasivas**. Cuando se vayan a utilizar tecnologías que se consideran especialmente invasivas con la privacidad como la videovigilancia a gran escala, la utilización de aeronaves no tripuladas (drones), la vigilancia electrónica, la minería de datos, la biometría, las técnicas genéticas, la geolocalización, o la utilización de etiquetas de radiofrecuencia o RFID) (especialmente, si forman parte de la llamada internet de las cosas) o cualesquiera otras que puedan desarrollarse en el futuro.

- **Cesiones o transferencias internacionales de datos.** Cuando se cedan o comuniquen los datos personales a terceros y, en particular, siempre que se pongan en marcha nuevas iniciativas que supongan compartir datos personales con terceros que antes no tenían acceso a ellos, ya sea entregándolos, recibiéndolos o poniéndolos en común de cualquier forma.
- **Cesiones o transferencias internacionales de datos.** Cuando se vayan a transferir los datos a países que no forman parte del Espacio Económico Europeo (Espacio Económico Europeo) y que no hayan sido objeto de una declaración de adecuación por parte de la Comisión Europea o de la Agencia Española de Protección de Datos.
- **Tratamientos con nuevas categorías de datos / Determinación de perfiles.** Cuando se enriquezca la información existente sobre las personas mediante la recogida de nuevas categorías de datos o se usen las existentes con nuevas finalidades o en formas, que antes no se usaban, en particular, si los nuevos usos o finalidades son más intrusivos o inesperados para los titulares.
- **Tratamientos con datos de menores.** Cuando se lleve a cabo un tratamiento significativo no incidental de datos de menores o dirigido especialmente a tratar datos de estos, en particular si tienen menos de catorce años.

La aplicación de cada factor de riesgo debe ser graduada para modular de esta manera el resto de parámetros del análisis, a modo de ejemplo se detalla cómo puede hacerse esta modulación en la *Tabla 8. Factores de riesgo y su ponderación para determinar los riesgos de impacto en la privacidad y las salvaguardas a implantar.*

| | **Analítica de datos interna (big data)** | **Tratamientos masivos** | **Tratamientos con datos especialmente protegidos.** | **Analítica de datos (para terceros)** | **Tecnologías invasivas** | **Cesiones / Transferencias internacionales de datos** | **Tratamientos con nuevas categorías de datos / Determinación de perfiles** | **Tratamientos con datos de menores** |
|---|---|---|---|---|---|---|---|---|
| **100 %** | Existen análisis estadísticos de determinación de patrones y se definen elementos que se salen del patrón y además estos datos son publicados. | El tratamiento afecta a más de 10.000.000 personas. | Más del 30% de los registros son datos especialmente protegidos. | Se ceden datos personales no anonimizados | Uso de técnicas genéticas | Se ceden datos personales a países manifiestamente transgresores. | Se pueden deducir gustos sexuales, ideas políticas o religiosas. | Más del 30% de los registros son objeto del tratamiento. |
| **60%** | Existen análisis estadísticos de determinación de patrones y se definen elementos que se salen del patrón. | El tratamiento afecta a más de 1.000.000 personas. | Menos del 30% de los registros son datos especialmente protegidos. | Se ceden datos personales pseudo anonimizados | Uso de drones | Se ceden datos personales a países orientales. | Existen nuevas finalidades incompatibles con el responsable del tratamiento. | Menos del 30% de los registros contienen datos de menores. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **30%** | Se hacen estudios estadísticos dinámicos (se determinan patrones de riesgo). | El tratamiento afecta a más de 100.000 personas. | Menos del 10% de los registros son datos especialmente protegidos. | Se ceden muestras de datos | Uso de RFID | Se ceden datos a EEUU, Australia, Sudamérica | Existen nuevas finalidades compatibles con el responsable del tratamiento. | Menos del 10% de los registros contienen datos de menores. |
| **10%** | Se hacen estudios estadísticos estáticos. | El tratamiento afecta a más de 10.000 personas. | Menos del 2% de los registros son especialmente protegidos. | Se ceden datos agregados. | No hay técnicas invasivas. | Se ceden datos a países de la Unión Europea. | La definición actual de finalidades ya está recogida en el tratamiento. | Menos del 2% de los registros contienen datos de menores. |
| **0%** | No hay datos personales | El tratamiento afecta a menos de 10.000 personas. | No han tratamientos | No hay cesiones. | No hay técnicas invasivas | No hay cesiones. | No hay nuevas finalidades | No hay tratamientos |

*Tabla 8. Factores de riesgo y su ponderación para determinar los riesgos de impacto en la privacidad y las salvaguardas a implantar.*

### 4.3.3. RIESGOS DE IMPACTO EN LA PRIVACIDAD

Los riesgos de seguridad específicos se agrupan en los siguientes capítulos:

**Carencia de legitimación en el tratamiento de los datos**

Consiste en que el responsable del tratamiento trata los datos sin estar autorizado por una ley y, en este caso, sin cumplir con los requisitos necesarios que le legitimen para el tratamiento de éstos.

En particular, incluye los siguientes riesgos:

- Tratamiento no autorizado por ley y sin contar con el consentimiento del titular.
- Cesiones de datos no autorizados por ley y sin contar con el consentimiento del titular.
- Transferencias internacionales de datos fuera del Espacio Económico Europeo sin cumplir con los requerimientos legales o sin cumplir con las suficientes medidas de seguridad.

**Vulneración de derechos de los titulares**

Consiste en la realización por parte del responsable del tratamiento de acciones o, en su caso, no dar cumplimiento a requisitos actualmente demandados por la normativa de protección de datos que puedan suponer una vulneración o ataque a los derechos de los titulares.

En particular, incluye los siguientes riesgos:

- **No se informa** al titular del dato del tratamiento y la cesión de sus datos.
- **No se solicita el consentimiento del titular para el tratamiento y cesión de sus datos**: No se está solicitando el consentimiento de los titulares para la cesión o tratamiento de sus datos cuando no hay una ley que lo autorice.
- **No se da cumplimiento al derecho a la portabilidad de datos**: No se está realizando las acciones necesarias para hacer efectivo el derecho o bien no se han arbitrado medios en la organización para llevarlo a cabo.
- **No se da cumplimiento al derecho al olvido**: No se está llevando a cabo en la organización las acciones para hacer efectivo el derecho o bien no se han arbitrado medios en la organización para llevarlo a cabo.

- **No se da cumplimiento al ejercicio de derechos ARCO**: No se está informando ni se ha previsto un medio para hacer efectivo el ejercicio de los derechos ARCO (tales como dirección donde dirigir las solicitudes, medio a utilizar para ejercerlo, etc.). La organización no dispone de procedimientos para hacer efectivo el ejercicio de los derechos de los titulares en la organización.
- **Impugnación de valoraciones**: Se pueden tomar decisiones significativas en relación al titular que produzcan efectos jurídicos y que se basen únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

**Incumplimiento del principio de calidad de datos**

El responsable del tratamiento no aplica en relación al tratamiento de los datos, los requerimientos del principio de calidad de los datos.

En particular incluye los siguientes riesgos:

- **Finalidades indebidas o excesivas para el tratamiento de datos autorizado**: Se tratan los datos para finalidades incompatibles, indebidas o que exceden de las finalidades del tratamiento expresamente autorizadas por una ley o para las que se han recopilado los datos.
- **No se aplican políticas de actualización periódica de la información**: Los datos no se actualizan periódicamente o bien no se aplican políticas de actualización periódica de la información, garantizando que los datos sean exactos y completos.
- **No se aplican políticas periódicas de cancelación / expurgo de la información**: No se aplican o bien no se han definido políticas periódicas de cancelación o expurgo de la información, conservando únicamente los datos necesarios.

**Fugas de información**

La información titularidad de la organización y que es objeto de tratamiento es difundida de manera deliberada o maliciosa a terceros no autorizados.

En particular incluye los siguientes riesgos:

- **Accesos no autorizados**: No se han implantado medidas de control de acceso lógico a los sistemas así como medidas de control de acceso físico a las instalaciones donde se ubican éstos y la información/documentación
- **Incumplimientos del deber de secreto**: No se han firmado cláusulas de compromisos de deber secreto o confidencialidad en el tratamiento de la información ni por parte de personal interno ni por parte del personal externo que va a participar en el tratamiento.

**Deficiencia en el control y gestión de tratamientos externalizados**

El responsable del tratamiento no aplica las medidas necesarias que garanticen el control adecuado de tratamientos cuya gestión de manera total o parcial se haya delegado en terceros o prestadores de servicios.

En particular incluye los siguientes riesgos:

- **Deficiencias en los contratos de encargo**: No hay elaborado un modelo de contrato para la prestación de los servicio/s que vayan a estar presentes en el tratamiento y que cumpla con los requerimientos de la ley tanto para el caso de que el prestador vaya a acceder a datos personales como si no va a acceder.
- **Falta de diligencia o capacitación del encargado del tratamiento**: No se ha incluido en el contrato de prestación de servicios cláusulas específicas que garanticen el control del prestador, en torno a la capacitación, diligencia, compromiso de confidencialidad y prestación del servicio con unas adecuadas condiciones de calidad (inclusión de acuerdos de nivel de servicio, etc. ).

- **Subcontrataciones no autorizadas por ley**: No inclusión en los contratos de prestación de servicios de una cláusula por la cual se prohíba la subcontratación de servicios por parte del encargado del tratamiento sin contar con la autorización expresa del responsable del tratamiento. No se efectúa por el responsable un control de estas subcontrataciones.
- **Falta de control efectivo por el responsable de la prestación del servicio**: El responsable del tratamiento está llevando a cabo un control efectivo de la prestación del servicio realizado por el Encargado que garantice que se ajusta a la LOPD en el tratamiento y manejo de este tipo de datos.

**Falta de formación y conocimiento experto en materia de protección de datos**

Desconocimiento de la normativa de protección de datos tanto por los responsables como los que participan en la gestión del tratamiento.

Los responsables internos y el personal que participa en el tratamiento de la información referida al tratamiento titular desconocen el contenido y las implicaciones de la LOPD/RGPD en relación al tratamiento.

### 4.3.4. MEDIDAS QUE MITIGAN LOS RIESGOS DE PRIVACIDAD

Los riesgos anteriores se mitigan con un conjunto de medidas de seguridad de tipo informático, legal y organizativo. Cada una de ellas mitiga en un grado variable parte de los riesgos anteriores.

Los grupos de medidas de seguridad se han basado en las medidas del Esquema Nacional de Seguridad y en la guía de evaluación de impacto en la privacidad de la AEPD.

**Cumplimiento controles de seguridad**

Esta es la relación de medidas del ENS que aplican a este caso. Por cada una se menciona su referencia del anexo II del RD 3 / 2010, por lo que no se comenta más aquí:

- Identificación/ autenticación (op.acc. 5 ENS y RD1720/2007 ART.93 y 98).
- Proceso de autorización (org.4 ENS).
- Segregación de funciones y tareas (op.acc.3 ENS).
- Control de acceso (op.acc.6 ENS), RD1720/2007 ART.91).
- Configuración de seguridad (op.exp.2 ENS)
- Cifrado de información almacenada (RGPD)
- Protección frente a código dañino (op.exp.6 ENS).
- Protección de las instalaciones e infraestructuras (mp.if ENS y RD1720/2007 ART. 99).
- Caracterización del puesto de trabajo (mp.per.1 ENS).
- Gestión y distribución de soportes y documentos (RD1720/2007 ART.92, 97 y 101)/ (mp.si.2 ENS).
- Trazabilidad (ENS)/ Registro de Accesos (RD1720/2007 ART. 103).
- Pruebas con datos reales (RD1720/2007 ART.94.4).
- Protección de telecomunicaciones (RD1720/2007, ART.104).
- Auditorías (ART. 34, RD 3/2010 y ART.96 RD1720/2007).
- Gestión, registro y notificación incidencias/violaciones de seguridad (RD1720/2007, ART.90 y 100, ART.33 y 34 RGPD).
- Ficheros temporales (ART.87 RD1720/2007).
- Gestión documentación (ART.105 a 114 RD1720/2007).
- Aplicación de medidas de seudonimización (RGPD).

**Legitimación del tratamiento**

En relación a este ámbito se contemplan las siguientes medidas:

- **Cláusulas informativas**: Elaboración de cláusulas que informen de las finalidades afectadas por el tratamiento analizado así como la cesión de sus datos. Arbitraje de los medios necesarios para la difusión y divulgación de estas cláusulas entre los titulares
- **Gestión del consentimiento**: Elaboración y almacenamiento de Cláusulas de solicitud del Consentimiento tanto respecto al tratamiento como a la cesión de los datos de los titulares cuando una ley no lo autorice expresamente. La solicitud del consentimiento será para todas las finalidades del tratamiento y no autorizadas por una ley. Arbitrar los medios necesarios para la difusión y divulgación de estas cláusulas entre los titulares.
- **Legitimación Transferencias internacionales y cesiones de datos**: Solicitar autorización formal a la autoridad competente para la realización de las transferencias fuera del Espacio Económico Europeo. Implantación de medidas de seguridad requeridas por ley para la realización de las cesiones o transferencias internacionales que pudieran resultar afectadas.

**Cumplimiento con los derechos de los titulares**

En relación a este ámbito se contemplan las siguientes medidas:

- **Derecho de información.** Implantación de un procedimiento para hacer efectivo el derecho de información en el plazo y con la calidad requerida.
- **Solicitud del consentimiento** Implantación de un procedimiento para que el titular del dato preste el consentimiento a sus tratamientos en el plazo y con la calidad requerida.
- **Derechos ARCO:** Elaboración de un procedimiento para hacer efectivo el ejercicio de los derechos ARCO de los titulares. Habilitar los medios necesarios para hacer efectivo su ejercicio (definiendo: lugar donde se centralice la recepción de las solicitudes, personal que va a tramitarlo y resolverlo, elaboración formularios para el ejercicio de estos derechos por parte de los titulares, etc.
- **Derecho a la portabilidad de datos:** Elaboración de procedimientos para hacer efectivo el Derecho a la portabilidad de los datos de los titulares. Implantación de las medidas para hacer efectivo dicho procedimiento.
- **Derecho al olvido.** Implantación de un procedimiento para hacer efectivo el derecho al olvido en el plazo y con la calidad requerida.

**Cumplimiento del principio de calidad de los datos**

En relación a este ámbito se contemplan las siguientes medidas:

- **Finalidades debidas y no excesivas:** Control periódico de los datos que forman parte del tratamiento titular con el objeto de que no se recopilen datos excesivos que sean incompatibles con las finalidades para las que autorizó o se recopiló la información.
- **Actualización periódica de la información:** Definición de políticas de actualización periódica de la información en relación al tratamiento titular. Implantación efectiva de esta política.
- **Cancelación periódica/Expurgo:** Definición de políticas de cancelación periódica y expurgo de la información relativa al tratamiento titular. Esta política contemplará medidas de eliminación segura de esta información. Implantación efectiva de dicha política.

**Sigilo**

En relación a este ámbito se contempla la siguiente medida:

- **Cumplimiento del deber de secreto:** Elaboración y firma de compromisos de confidencialidad en el tratamiento de la información en relación al tratamiento titular tanto por parte de personal interno como externo. Divulgación entre este personal de un documento con las funciones y obligaciones a cumplir en el tratamiento de los datos.

**Control y gestión tratamientos externalizados**

En relación a este ámbito se contemplan las siguientes medidas:

- **Cumplimiento requisitos legales de contratos de encargo:** Elaboración de modelos de contrato de servicios que cumpla con los requerimientos de la ley para el tratamiento titular, distinguiendo si se tratan de servicios en los que se va a acceder a datos de carácter personal o no (por ejemplo, artículo 12 de la LOPD, medidas de seguridad a aplicar en función del nivel de seguridad de los datos que se manejan, etc.) y que podrán ser complementarios a los ya establecidos en los Pliegos de Cláusulas Administrativas.
- **Diligencia, capacitación, confidencialidad de encargados de tratamiento**: Inclusión en el contrato de cláusulas específicas que garanticen el control en torno a la capacitación, diligencia, compromiso de confidencialidad y prestación del servicio con unas adecuadas condiciones de calidad (inclusión de acuerdos de nivel de servicio, etc.). Revisiones periódicas del servicio que garanticen que el prestador cumple con estos requisitos (acuerdos de nivel de servicio, etc.)
- **Subcontrataciones debidamente autorizadas**: Inclusión específica en el contrato de una cláusula por la cual se prohíba la subcontratación de servicios por parte del encargado del tratamiento sin contar con la autorización expresa del responsable del tratamiento. Realización de acciones de control y revisión periódica del control del servicio para identificación de este tipo de situaciones.
- **Cumplimiento de las obligaciones por el prestador:** Inclusión en el contrato de cláusulas específicas donde se detallen las obligaciones del prestador (tales como el mantenimiento del Documento de Seguridad, respuesta ejercicio de derechos, etc.). Control y revisión periódica a efectos prácticos del servicio para garantizar el cumplimiento de estas obligaciones.

**Formación en protección de datos**

En relación a este ámbito se contemplan las siguientes medidas:

- **Formación:** Impartición de cursos de formación en RGPD entre los responsables y el personal que va a gestionar los datos que forman parte del tratamiento titular.
- **Asesoramiento experto:** para el titular del tratamiento en materia de protección de datos personales.

## 4.4. FORMACIÓN, SENSIBILIZACIÓN Y CONCIENCIACIÓN

Por su carácter de responsable de seguridad, la GISS ya impulsa los planes de formación y concienciación relacionados con el ENS, por lo que está elaborando un curso de 5 horas para funcionarios de la Seguridad Social en el que se expliquen los siguientes apartados:

- Una introducción de los conceptos generales y los requisitos del RGPD.
- La aplicación del principio de seguridad activa (análisis de riesgos, evaluación de impacto en la privacidad, etc.)
- La aplicación de la seguridad de los tratamientos (seguridad desde el diseño y por defecto, la anonimización de los datos de prueba etc.).
- La aplicación concreta de lo anterior en procedimientos de trabajo.

El curso incluye unos ejercicios prácticos y un test final de conocimiento.

El curso comenzará en Marzo de 2018 en dos modos de impartición: presencial y eLearning (a través de pizarras virtuales y desde el puesto de trabajo de alumnos y tutores).

También se ha primado el que parte de los tutores sean responsables de unidades provinciales de informática, pues ellos son conocedores de los problemas concretos que diariamente se dan en las oficinas de la organización. De esta manera, la estrategia es dar contenidos lo más concretos y prácticos posibles.

La concienciación va a ser impartida dentro de los canales habituales en la organización, que consisten principalmente en noticias sencillas y atractivas que el Comité de Seguridad aprueba y que se envían periódicamente a todos los trabajadores de la organización.

## 4.5. IMPLANTACIÓN DE MEDIDAS TÉCNICAS

### 4.5.1. SEGURIDAD DESDE EL DISEÑO Y POR DEFECTO

La GISS ha trabajado también en la implantación de las nuevas medidas técnicas que demanda el RGPD. En concreto, el artículo 25 del RGPD se centra en la protección de datos desde el diseño y por defecto estableciendo:

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

La GISS ya lleva años sometiendo a los nuevos tratamientos a controles de seguridad en el ciclo de vida (esta es otra de las exigencias del ENS). En concreto:

- Se hacen consultas en la fase de análisis, en la toma de requisitos, de los niveles de seguridad de los datos para confirmar que están previstas las medidas exigidas por la legislación (por ejemplo, la generación y explotación de rastros de accesos para datos de nivel alto).
- Se revisa en la fase de diseño que los programas informáticos llaman a los módulos informáticos comunes en seguridad para confirmar que se definen los módulos.
- Se prueban los programas en la fase de entrega a producción para que sean robustos a las vulnerabilidades más comunes (en entorno web por ejemplo las recogidas en OWASP[2]).
- Se hacen varios test de intrusión[3] para probar las fortalezas de los entornos informáticos más expuestos en internet y además también algunos de los internos

En este aspecto queda pendiente:

- Integrar las evaluaciones de impacto en la privacidad en la fase de análisis para determinar si afectan al tratamiento implicado y garantizar así que cuando esta aplicación informática pase a producción ya tiene implementadas las medidas adecuadas
- Una definición de los plazos de conservación de la información del tratamiento.
- Una revisión en la fase de mantenimiento de que las medias decididas de impacto en la privacidad se están cumpliendo efectivamente.

### 4.5.2. SEUDOANONIMIZACIÓN DE DATOS

La GISS también ha trabajado en la implantación dentro de la organización de esta medida técnica reconocida por el RGPD en su artículo 25 y 32.

[2] OSASP (https://www.owasp.org/index.php/Main_Page) es una organización sin ánimo de lucro que cada 3 años publica el llamado "TOP 10" de vulnerabilidades más comunes en aplicaciones web.

[3] En un test de intrusión (también llamado "hacking ético") se contrata a un equipo de expertos de seguridad para atacar un sistema de manera controlada y con el único ánimo de detectar puntos débiles para que posteriormente puedan ser corregidos.

En este sentido, ha definido una metodología de evaluación de riesgos en la seudoanonimización de datos muy parecida a la evaluación de impacto en la privacidad, pero con diferentes riesgos, factores de riesgos, medidas de seguridad y grado de implantación, que no ha sido desarrollado en este documento.

Esta metodología ha sido elaborada en aplicación de la guía "Orientaciones y garantías en los procedimientos de anonimización de datos" publicada por la AEPD.

Se han acotado los supuestos se debería aplicar esta medida, como:

- Tratamientos con fines estadísticos, investigaciones de mercado laboral, etc.
- Tratamientos con fines históricos y de registro, etc.

### 4.5.3. CIFRADO DE LA INFORMACIÓN

Una de las principales medidas de carácter técnico que identifica el nuevo RGPD en su artículo 32 es el cifrado de la información. En concreto establece:

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

En relación al cifrado, desde la GISS se identificaron los siguientes ámbitos sobre los cuales aplica esta medida:

- Cifrado de correos.
- Cifrado de discos virtuales.

Cifrado de los correos: desde la GISS se ha impulsado de manera centralizada el cifrado de los documentos que se adjuntan a correos, en los casos en los que a través de estos documentos se envía información con datos de nivel alto. Para ello, se ha identificado una herramienta, disponible para todo el personal de la organización a través del cual se está haciendo efectivo, el que los empleados puedan enviar este tipo de información de manera cifrada.

Cifrado de discos virtuales: también desde la GISS se han remitido instrucciones específicas a los usuarios para el cifrado de la información contenida en este tipo de soportes en los casos en los que a través de los mismos se vaya a albergar información sensible. Desde la GISS se han facilitado herramientas para el adecuado cifrado de la información contenida en estos soportes. Así mismo, se ha dado difusión a la existencia de este tipo de herramientas.

Está en estudio la utilización de estas técnicas en los sistemas de información, teniendo en cuenta sus implicaciones técnicas y económicas. Se reconoce un especial interés para los casos de "notificaciones de violaciones de seguridad".

### 4.5.4. NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD

El art. 33 y 34 del nuevo RGPD establece que, en caso de que se produzca una violación de la seguridad que afecte al tratamiento de datos personales del afectado/s y constituya un riesgo para los derechos y las libertades de las personas físicas, dicha violación se deberá comunicar a la autoridad de control en el plazo de 72 horas así como, en su caso, al interesado sin dilación indebida.

Para la implantación de esta medida, desde la GISS se impulsó la modificación del procedimiento de gestión de incidentes existente en la organización con el objeto de que albergara los nuevos requerimientos que demandaba el RGPD.

Así mismo, se impulsó en la organización la utilización de una herramienta centralizada para la gestión de las incidencias.

A continuación se realizaron acciones específicas de divulgación entre el personal que participa en la gestión y resolución de este tipo de incidencias en torno a las acciones y medidas a implantar en caso de que se produzcan este tipo de incidencias, así como se dio a conocer esta herramienta y sus funcionalidades.

### 4.5.5. PLANES DE CONTINUIDAD DE LA ORGANIZACIÓN

El artículo 32. 1 c) del nuevo RGPD establece que:

"*Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros…….*la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

En este sentido ya existe un plan de continuidad de negocio que afecta a la Seguridad Social que se sustenta en dos Centros de Proceso de Datos, que actúan como principal y secundario en modalidad activo-pasivo. En la actualidad se trabaja para poner los servicios en modo activo-activo y se tiene como estrategia llegar a tener los dos centros como principales trabajando de forma colaborativa y absorber la carga de trabajo uno de ellos ante contingencias.

Baste decir que se han tenido en cuenta, dentro de los escenarios de contingencia (un escenario de contingencia se define en el contexto de este informe como el conjunto de amenazas de seguridad cuya actuación en caso de materialización está compuesta de un conjunto de acciones común) se ha incluido el de fuga de información.

### 4.5.6. AUDITORIAS DE CUMPLIMIENTO

Como ya se ha comentado al comienzo de este análisis la Seguridad Social es sometida cada dos años a dos tipos de auditorías (LOPD y ENS) en años alternos.

Estas auditorías por parte de la GISS van a ser unificadas con las de cumplimiento del RGPD, aspecto que se ha facilitado con las nuevas normas de cumplimiento del ENS y su adecuación al RGPD. Esto supondrá un ahorro de costes y de esfuerzo ya que se pueden realizar auditorías únicas y que cada dos años verifiquen el cumplimento de ambas normas legales que son ya estándares de facto.

El resultado de cada uno es un conjunto de "no conformidades" para ser seguidas y corregidas de manera continua antes de la llegada de una nueva auditoría. Las más importantes serán integradas en proyectos de adecuación con duración bienal.

De esta manera el seguimiento de estas no conformidades se integra en planes continuos de mejora de la seguridad y se hacen compatibles con nuevos requisitos que puedan surgir entre tanto con nuevos proyectos informáticos que impliquen innovaciones tecnológicas (como los de analítica de datos, datos biométricos, etc.,) que impliquen análisis de impacto en la privacidad.

### 4.5.7. USO DE HERRAMIENTAS CENTRALIZADAS PARA LA ADAPTACIÓN AL RGPD

La GISS es consciente de que en una organización tan grande y compleja como la Seguridad Social, para la adecuada implantación de las medidas requeridas por la nueva norma es necesario contar con herramientas, normas y procedimientos que ayuden en las labores de coordinación y simplificación de las medidas a implantar A continuación se detallan algunas de las herramientas que la organización ha incorporado para mejorar la gestión en la implantación de esta nueva normativa:

- El modelo unificado de controles de seguridad, ya comentado anteriormente.
- Utilización del Portal de la organización, intranet etc., para la coordinación de la formación en Seguridad que demanda esta Normativa, publicación de píldoras informativas, publicación de la normativa, políticas y procedimientos definidos para dar cumplimiento a la norma, etc.
- Definición y desarrollo de una herramienta centralizada para la realización de las Evaluaciones de Impacto en la organización.
- Herramientas para la gestión centralizada del ejercicio de los derechos por parte de los afectados (sede electrónica).

- Herramienta centralizada para la gestión y comunicación/notificación de las incidencias/ violaciones de seguridad que se producen en la organización (LUCIA).
- Herramienta centralizada para la notificación y registro de los tratamientos LOPD en la organización.
- Herramientas para la gestión de los rastros y revisión de los accesos relativos a los sistemas afectados.
- Herramienta centralizada para la realización de los Análisis de Riesgos basada en una metodología universalmente reconocida.

## 4.6. VALORACIÓN DE LA HERRAMIENTA PILAR PARA ANÁLISIS DE RIESGOS

PILAR es la herramienta de cálculo de riesgos promovida por el Centro Criptológico Nacional (CCN) y que sirve de soporte a la metodología Magerit, de análisis y gestión de riesgos de seguridad. Esta herramienta está implantada desde hace varios años en España y su uso es habitual en las administraciones públicas.

La metodología de riesgos debe ser adaptada al RGPD para incluir amenazas, salvaguardas y otros aspectos relacionados con la privacidad y el complimiento normativo derivado de este estándar de seguridad. Uno de los pasos necesarios para ello es la adaptación de PILAR, pero incluyendo los aspectos tradicionales de seguridad de la información (relacionados con la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad).

El CCN ha elaborado por ello una versión de la herramienta que incluye la adaptación a estos aspectos nuevos. La GISS ha recibido esta versión y con ella ha realizado las siguientes acciones:

- Confeccionar un ejemplo completo de tratamiento de datos personales ficticio, incluyendo con altos riesgos de seguridad, y aplicarlo al cálculo de la herramienta.
- Enviar al CCN los resultados, una relación de dudas y aspectos a mejorar en la herramienta.
- Valorar el modo de empleo de la herramienta para que sea útil para administraciones públicas.

Las conclusiones fueron comunicadas al CCN y han sido las siguientes:

- Los resultados finales de PILAR, como herramienta de cálculo de riesgos, deben aportar la información suficiente para poder priorizar la inversión en medidas de seguridad (ver la *figura 10: Las entradas y salidas de PILAR necesarias para poder priorizar el presupuesto de seguridad*:
  - La lista ordenada de los activos con mayor riesgo intrínseco.
  - La lista ordenada de las amenazas con mayor riesgo intrínseco.
  - La relación de medidas de seguridad que deben ser realizadas teniendo en cuenta su coste y el riesgo que reducen.
  - La lista ordenada de escenarios de contingencia con mayor riesgo intrínseco.
- PILAR debe poder permitir a los analistas de riesgos conocer el motivo por el que se obtienen los resultados anteriores. En concreto, el motivo por el que un riesgo determinado es alto (basándose en valores previos del valor de los activos afectados, la probabilidad de materialización de una amenaza y la degradación del activo en caso de que suceda).

Y la mejor manera de cumplir con los requisitos anteriores es mediante el desarrollo de uso de PILAR para hacer análisis y gestión de riesgos. A partir de ella una administración pública debería poder utilizar la herramienta centrándose en los pasos concretos a dar y qué opciones usar de PILAR.

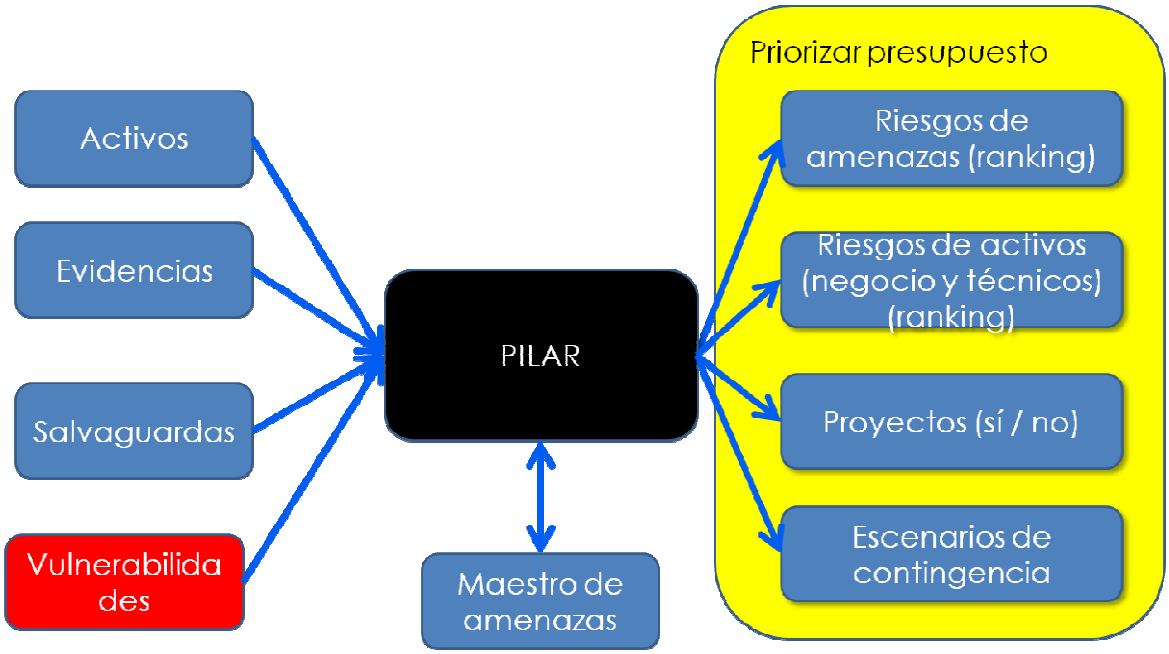


*Figura 10: Las entradas y salidas de PILAR necesarias para poder priorizar el presupuesto de seguridad.*

# 5. EXTENSIÓN DEL PROYECTO A OTRAS ADMINISTRACIONES PÚBLICAS

El proyecto de implantación del nuevo RGPD permite su aplicación a otras administraciones públicas y empresas privadas.

Las razones son las siguientes:

- A través de una herramienta se gestiona, centraliza y coordina la seguridad que aplica a toda una organización, permitiendo realizar una integración de los distintos controles que son aplicables a una organización desde el punto de vista de la seguridad.
- La implantación se lleva a cabo a través de procedimientos fácilmente trasladables. Lo que es exclusivo de cada organización son los departamentos que ejercen las funciones de estos procedimientos. (DPD, responsables de tratamiento etc.).
- Se identifican herramientas para la implantación cuya referencia y posible utilización pueden ser fácilmente trasladables a otras organizaciones de rango similar (herramientas de Análisis de Riesgos, gestión de los incidentes, registro de tratamientos, etc.).
- En este caso, en el caso de las Administraciones Públicas, la integración desde el punto de vista de la seguridad se centra básicamente en la integración de normativas ya conocidas, como el Esquema Nacional de Seguridad, la actual LOPD y su normativa de desarrollo y el nuevo RGPD entre otros.

### 5.1.1. EJEMPLO DE APROVECHAMIENTO DE ESTÁNDARES DE SEGURIDAD

El modelo unificado de controles de seguridad aporta una reutilización de las tareas de adecuación en otros estándares de seguridad. Supongamos por ejemplo una organización que ya tiene un grado de cumplimiento medido en el ENS, la LOPD y el RD de desarrollo de la LOPD de, por ejemplo:

| | Grado de cumplimiento |
|---|---|
| **Estándar de seguridad** | Aislado |
| ENS | 60% |
| LOPD | 80% |
| RDLOPD | 80% |

*Tabla 9. Un ejemplo de cumplimiento en una organización*

Sólo con esos datos ya es posible obtener el grado de cumplimiento del RGPD como la media ponderada de los datos anteriores:

| | Controles | | Grado de cumplimiento | |
|---|---|---|---|---|
| **Estándar de seguridad** | **Número** | **%** | Aislado | Ponderado |
| ENS | 116 | **66%** | 60% | 39% |
| LOPD | 15 | **8%** | 80% | 7% |
| RDLOPD | 46 | **26%** | 80% | 21% |
| **RGPD** | 177 | **100%** | | **67%** |

*Tabla 10. Un ejemplo del grado de cumplimento RGPD en relación con el de estándares de seguridad relacionados.*

Obsérvese la influencia que supone el ENS, mayor incluso que la LOPD y el RDLOPD. Este dato, puede sorprender, pero se explica por gran carga de requisitos de seguridad que implica su implantación y que son comunes en gran medida a los nuevos que deben contemplarse para el cumplimiento RGPD.

# 6. CONCLUSIONES

Actualmente la Seguridad Social ha conseguido a partir de los trabajos de la iniciativa de la GISS la designación de un DPD, un plan de proyectos para desarrollar la adecuación, un sistema de seguimiento basado en controles de cumplimiento, procedimientos de cumplimiento y una relación importante de tareas técnicas y normativas a cumplir que debe ser completada y aprobada por todas las Entidades Gestoras y Servicios Comunes de la Seguridad Social bajo la supervisión del DPD.

El trabajo inicial ha comenzado, pero quedan otras tareas, como desarrollar los canales y aplicaciones informáticas que darán soporte a nuevos procedimientos de cumplimiento (por ejemplo el derecho de portabilidad o el canal de atención que el DPD prestará a los responsables de tratamiento y a los titulares de los datos).

Además, otros desafíos deberán ser resueltos en próximas fechas, como la coordinación del responsable de seguridad y el Comité de Seguridad con el DPD, sabiendo que tienen competencias (los dos primeros en el entorno del ENS y el último del RGPD) con aspectos comunes.

No obstante, el RGPD se presenta como el estándar de seguridad que integra la actual LOPD y su reglamento de desarrollo y el ENS y con el estilo de los estándares ISO 27001 e ISO 27002. Vale la pena invertir esfuerzos porque su cumplimiento es, sin duda, una línea estratégica acertada porque confluirá sin duda en una mejor seguridad y, con ella, en una mejor prestación de servicio por parte de las administraciones públicas a sus ciudadanos.