LA GESTIÓN DE LA PRIVACIDAD EN EL INSS:

Haciendo realidad el enfoque 360°

INSTITUTO NACIONAL DE LA SEGURIDAD SOCIAL

ÍNDICE

RESUMEN EJECUTIVO

El Instituto Nacional de la Seguridad Social es una entidad gestora dotada de personalidad jurídica propia, dependiente de la Secretaria de Estado de la Seguridad Social y Pensiones, que basa prácticamente la totalidad de su actividad en el tratamiento de datos personales como forma de cumplir con la misión y competencias encomendadas.

Desde que se tuvo conocimiento de la existencia de trabajos orientados a la adopción de un nuevo marco normativo, de alcance europeo, de garantía de la protección de la privacidad de los datos personales, la Entidad llevó a cabo una tarea de acercamiento y estudio de las principales novedades avanzadas por la doctrina y la prensa especializada. Y una vez publicado el Reglamento (UE) 2016/679, de 27 de abril de 2016 (RGPD), el periodo de la demora de su aplicación directa en España se aprovechó para llevar a cabo una intensa actividad de análisis y ponderación de las actuaciones a las que la Entidad venía obligada.

En el marco del **PLAN ESTRATÉGICO DEL INSS PARA EL PERIODO 2016-2018**, y de acuerdo con el **MODELO DE EXCELENCIA** en el que este Insituto se apoya para la mejora constante de sus procesos y servicios, el conocimiento de la nueva filosofía europea de la protección de la privacidad, y de las nuevas exigencias para los sujetos responsables, condujeron a la determinación de los resultados que se debían alcanzar en las distintas parcelas en las que el INSS vertebra su actuación, a la adopción del enfoque que se consideró más adecuado para lograr los resultados pretendidos, y al despliegue de las actividades de adaptación en todas las áreas relevantes. El resultado de estas actuaciones, coordinadas por la Secretaría General de la Entidad, fue y es objeto de evaluación y revisión constante, dando lugar a un modelo circular de actuación, al que se ha dado en llamar: enfoque 360º, al que se alude en el título de este trabajo. Tener "ojos" y "manos" en toda la organización e interiorizar la filosofia del RGPD y pensar en términos de protección de datos a la hora de acometer nuestra actividad, de forma transversal.

En efecto, la adopción de este paradigma, no es solo el trasunto del modelo de excelencia, antes citado, sino una apuesta necesaria por la especificidad de la materia y por las peculiaridades de la organización. La garantía de que se cumple con lo establecido, de que respetamos la privacidad de las personas a quienes pertenecen los millones de datos personales que manejamos, pasa por articular una dinámica “de barrido” constante, mediante la que, como si de un faro se tratase, se controla sin ángulos muertos el cumplimiento de las previsiones sobre privacidad.

A través de las páginas que siguen se efectúa una exposición de la proactividad de la Entidad, de cómo ha interiorizado el principio de responsabilidad activa, preconizado por el RGPD, de las buenas prácticas adoptadas, y de los mecanismos de control establecidos. Todo ello, siguiendo un relato en el que se escenifica la superación de distintas fases o etapas. La multitud de implicaciones e interacciones de los distintos elementos en juego hace que algunas fases sean presupuesto de la siguiente, en tanto que otras se desarrollen en paralelo con actuaciones

que en la exposición parecen precederlas. Esta es la dificultad y el atractivo de un reto como el que se describe.

Así, tomando como punto de partida lo que se ha dado en llamar **FASE EXPERIENCIA**, que incorpora el conocimiento y la práctica adquiridos en el periodo anterior a la entrada en vigor del RGPD, y con apoyo en los que se consideran los pilares de la organización y los valores que impregnan nuestra cultura, la exposición recorre las actuaciones llevadas a cabo en este camino sin fin.

La **FASE DE ANÁLISIS DEL IMPACTO DEL RGPD** y la **FASE NORMATIVA,** está dedicada fundamentalmente al análisis del impacto en las actividades de nuestra organización del RGPD y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) así como al diseño y regulación de las estructuras y soportes organizativos en que se sustentan: Delegado de Protección de Datos (DPD), Comisión de Protección de Datos y Subdelegado de Protección de Datos (SPD). La **FASE DE PLANIFICACIÓN ESTRATÉGICA Y OPERATIVA**, destaca fundamentalmente por la constitución y el comienzo de las actividades del Grupo de Protección de Datos del INSS. En la **FASE DE ACCIÓN**, se fijaron las concretas actuaciones a llevar a cabo para cumplir con los requerimientos del RGPD, y se operacionalizaron en un diagrama que permitía conocer en cada momento el grado de consecución de las tareas identificadas. La **FASE DE GESTIÓN DEL CONOCIMIENTO, FORMACIÓN Y CONCIENCIACIÓN** comprende todas las actuaciones dirigidas a enseñar, a concienciar, a formar e ilusionar al personal con el nuevo marco normativo. La **FASE GESTIÓN DE LA SEGURIDAD Y PRIVACIDAD** engloba todas las actividades articuladas para cumplir los requerimientos del Esquema Nacional de Seguridad, que constituyen el presupuesto de la garantía de la privacidad.

El círculo se cierra con la **FASE DE CONTROL Y REVISIÓN**, último punto de este "barrido" constante, de este enfoque 360º que se constituye, a su vez, en punto de partida de planificación de nuevas actuaciones.

Por último, al final de esta memoria, como muestra de la proactividad y compromiso con la protección de la privacidad de nuestro Instituto, se destacan **TRES BUENAS PRÁCTICAS** en tres áreas clave de la gestión de la Entidad con especial impacto en la protección de datos personales.

Nos resistimos a concluir este resumen ejecutivo del trabajo que se presenta al **PREMIO A LA PROACTIVIDAD Y BUENAS PRÁCTICAS** en el cumplimiento del RGPD y la LOPDGDD, sin citar unas palabras de Norbert Bilbeny, catedrático de ética en la Universidad de Barcelona y ensayista español:

> **"CUANDO "CONSIDERAMOS" PRESTAMOS ATENCIÓN A UNA COSA, NOS CONCENTRAMOS EN ELLA, Y PONEMOS, POCO O MUCHO, TODOS NUESTROS SENTIDOS EN ESTA OPERACIÓN... . EL INDIVIDUO "DESCONSIDERADO" NO HA APRENDIDO A PONDERAR, REACCIONA DE MANERA IMPULSIVA O ABRUPTA, O SIMPLEMENTE SIN PRESTAR ATENCIÓN A LOS SERES IMPLICADOS EN SU CONDUCTA".**

El INSS en su relación con todos los actores implicados en el ejercicio de sus competencias y, específicamente, en lo que afecta a la privacidad de los datos, trata de actuar como un individuo "considerado", atento a las consecuencias de su actividad, y dispuesto a adoptar con agilidad las medidas necesarias para garantizar los derechos reconocidos por el marco normativo. En ese **COMPROMISO** se instalan las actuaciones que se describen a continuación.

EL CONTEXTO DE LOS TRATAMIENTOS DE DATOS EN EL ÁMBITO DEL INSTITUTO NACIONAL DE LA SEGURIDAD SOCIAL

Para entender la relevancia de la protección de datos en el ámbito de la Seguridad Social y, en particular, en el que concierne al INSS, y con ello contextualizar la importancia del proceso de adaptación acometido, hay que tener en cuenta que nuestra Entidad Gestora basa prácticamente la totalidad de su actividad en un tratamiento intensivo de datos personales para hacer efectivas las competencias que tiene conferidas:

1. Reconocimiento y gestión de pensiones y subsidios del sistema de Seguridad Social,
2. Gestión del derecho a la asistencia sanitaria nacional e internacional, y
3. Las necesarias para el funcionamiento interno y gestión de nuestro personal.

Todo ello supone que debe gestionar y tener a su disposición una cantidad ingente de datos durante un prolongado periodo de tiempo.

Para ilustrarlo, de forma sucinta, podemos destacar los siguientes aspectos:

- En las bases de datos gestionadas directa y exclusivamente por el INSS, se alojan datos personales relativos a **MÁS DE 56 MILLONES DE PERSONAS** que se relacionan con el INSS a lo largo de toda su vida.
- Por tanto, su conservación, custodia y tratamiento se realiza durante el ciclo de vida de los datos más amplio posible desde el punto de vista de una persona, ya que supera de media los **82 AÑOS POR INDIVIDUO** (estimación realizada según datos de esperanza de vida media en España).
- Otra importante consecuencia de lo anterior es que los datos tratados durante ese amplio lapso temporal comprenden los momentos y hechos más relevantes que se producen en la **VIDA DE LAS PERSONAS,** comenzando desde el momento del nacimiento, el desarrollo de la vida laboral, todo lo relativo a la esfera familiar, las vicisitudes vitales que pueden afrontar tales como la enfermedad, la discapacidad, la incapacidad para el trabajo, la pérdida del empleo, el envejecimiento, la propia muerte o la de sus allegados, las derivadas de la carencia de ingresos o de su situación económica y laboral u otros supuestos como ser víctima de violencia de género o de actos de terrorismo...

Todos estos datos personales, además, se enriquecen con multitud de **INTERACCIONES E INTERRELACIONES** de bases de datos de otras entidades públicas y privadas. Lo que implica que, considerados en conjunto, pueden llegar a configurar un completo y pormenorizado perfil que engloba casi todos los aspectos fundamentales de un individuo, máxime si

[LA **PREOCUPACIÓN** POR LA PROTECCIÓN DE DATOS HA AUMENTADO NOTABLEMENTE DURANTE LA ÚLTIMA DÉCADA EN NUESTRA SOCIEDAD: POR UNA PARTE AUPADA POR LA MEJORA DE LA TÉCNICA DE MANERA EXPONENCIAL, QUE PERMITE CADA VEZ MÁS AMPLIOS Y COMPLEJOS TRATAMIENTOS QUE, UTILIZADOS DE MANERA INCORRECTA, SUPONEN CRECIENTES **AMENAZAS Y RIESGOS** MÁS CRÍTICOS QUE PUEDEN AFECTAR A CUALQUIER CIUDADANO DE A PIE; Y TAMBIÉN POR LA MAYOR CONCIENCIACIÓN SOBRE LOS **PELIGROS** QUE PUEDE LLEGAR A ENTRAÑAR]

tenemos en cuenta que esa información es el resultado de la confluencia de dos tipos de fuentes:

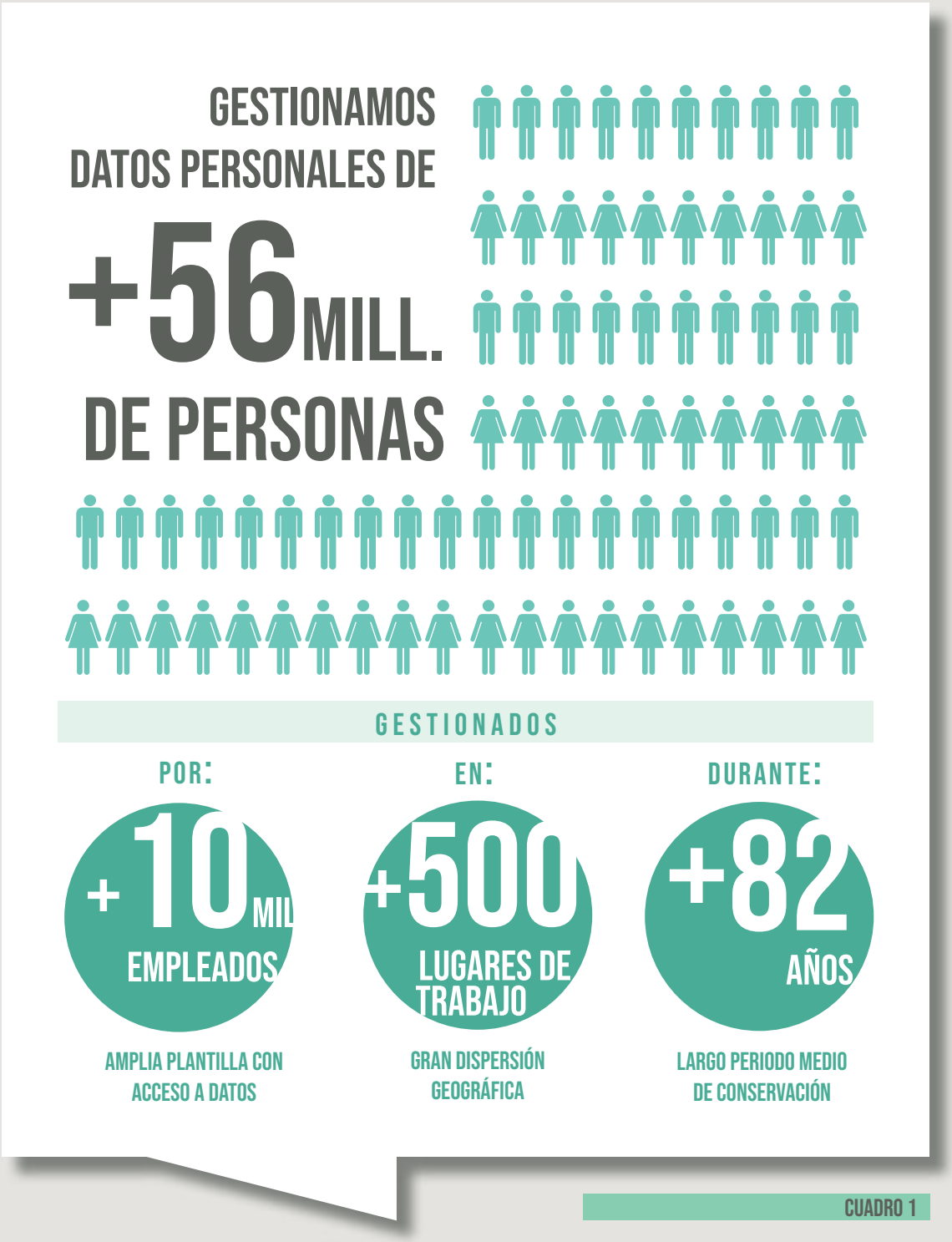
- Las **FUENTES DIRECTAS** ligadas con el cumplimiento de las competencias que nuestro Instituto tiene encomendadas.

EJ El reconocimiento y gestión de las prestaciones de incapacidad permanente, que implica el tratamiento de datos que desde la perspectiva de su protección, requieren de las máximas garantías, en particular: la salud pasada, presente y futura.

- Por otra, de **FORMA INDIRECTA**, se puede tener conocimiento de aspectos que van a ser fácilmente deducibles y que, aunque lejos de ser el objeto de tratamiento, se van a derivar del propio y necesario procesamiento de los datos para otras finalidades.

EJ La orientación sexual de una persona puede conocerse, no siendo objeto de tratamiento como tal, al ser deducible a partir de los datos necesarios para llevar a cabo el reconocimiento y trámite de un expediente administrativo de la prestación por nacimiento y cuidado de menor de dos interesados del mismo sexo.

Aparte de la variedad y especial naturaleza de los datos personales tratados por nuestra Entidad, tal y como se ha expuesto en los puntos anteriores, otro factor muy relevante que debemos destacar es la complejidad añadida para la gestión de la protección de datos derivada de la forma organizativa de este Instituto, ampliamente descentralizada y que ejerce su actividad a



CUADRO 1

través de una distribución de centros de trabajo y oficinas de atención al público muy capilarizada a lo largo y ancho de todo el territorio nacional.

Esto implica que la **DISTRIBUCIÓN GEOGRÁFICA DE LOS ACCESOS** a la citada información y la ubicación física de los ficheros en los que estos datos personales se conservan y tratan van a tener un impacto muy importante en materia de protección de datos añadiendo un plus de complejidad.

Concretamente, hay que tener en cuenta que nuestra Entidad tiene una estructura compuesta de una serie de unidades funcionales distribuidas por todo el territorio nacional, como se muestra en el mapa de la página siguiente **(CUADRO 2)**.

Esta organización, no sólo geográfica sino también funcionalmente descentralizada, plantea grandes retos, por ejemplo, a la hora de conseguir:

- una actuación homogénea en materia de protección de datos,
- una comunicación interna plenamente eficaz,
- una adecuada conservación de los datos personales o
- una correcta auditoría y control del acceso a éstos por parte de una plantilla propia de más de 10.000 efectivos distribuidos por todo el territorio o,
- de su consulta por parte de personal de otras entidades del ámbito de la Secretaría de Estado de la Seguridad Social y Pensiones (SESSP) (Tesorería General de la Seguridad Social (TGSS), Instituto de la Marina (ISM),…) o fuera de ella (AEAT, administración autonómica y local,…),
- otras interrelaciones con o sin acceso a datos personales con entidades privadas (entidades bancarias y cajas de ahorros,…),
- Contratación pública, encomiendas de gestión, encargos a medios propios personificados, convenios y acuerdos de colaboración, etc.

RETOS para la protección de los datos que no paran de aumentar si se tiene en cuenta la apuesta por lo digital:

- la **INTERCONEXIÓN DE LAS BASES DE DATOS** de las Administraciones Públicas (AAPP) y las crecientes comunicaciones electrónicas entre administraciones y con los propios interesados,
- los **ESPACIOS DE AUTOGESTIÓN DISPONIBLES 24X7** que permiten a los ciudadanos acceder a través de internet a sus datos y realizar trámites, como por ejemplo el proyecto Tu Seguridad Social, u otros grandes proyectos como la Tarjeta Social Digital, que progresivamente va incorporando datos de otras prestaciones externas a la Seguridad Social y situaciones personales de los ciudadanos, proporcionados y a la vez accesibles por numerosas administraciones,

Sin olvidar en este análisis otros aspectos que se derivan de cuestiones como la implantación de la **ADMINISTRACIÓN ELECTRÓNICA**:

- la creciente automatización y robotización de procesos o
- el uso del almacenamiento en la nube,
- la aplicación de técnicas de big data y mineria de datos aplicadas a nuestro ámbito,
- El crecimiento de la ciberdelicuencia,
- el auge del teletrabajo, o
- la dependencia de operadores privados radicados en paises con una regulación en materia de protección de datos más laxa que la europea.

1. Los servicios centrales ubicados en varios edificios en Madrid.
2. 52 direcciones provinciales ubicadas en las capitales de provincia.
3. Amplia red capilar de 430 oficinas de atención e información (CAISS)
4. Unidades de valoración médica de incapacidades
5. Naves e instalaciones destinadas al archivo de documentación en papel, cintas, microfilms y otros soportes magnéticos de almacenamiento masivo
6. Un Centro de Atención Telefónica y Telemática (CATT) atendido por medios propios, sito en Leganés (Madrid).

Red de centros de atención e información de la SS (CAISS)

CUADRO 2

EL INSTITUTO NACIONAL DE LA SEGURIDAD SOCIAL

CONTEXTO, MISIÓN, VISIÓN, VALORES Y SU COMPROMISO CON LA PRIVACIDAD

El INSS es una Entidad Gestora dotada de personalidad jurídica propia, dependiente del Ministerio de Inclusión, Seguridad Social y Migraciones, a través de la SESSP.

Para desarrollar adecuadamente su misión, el INSS cuenta con una importante infraestructura de gestión y ofrece a los ciudadanos servicios de atención e información multicanal, sometidos al principio de libre elección:

- **PRESENCIAL**, gracias a una amplia red periférica de 52 Direcciones Provinciales [DDPP] y CAISS 430 a junio de 2020
- **TELEFÓNICA**, mediante el CATT y varias unidades provinciales de atención telefónica
- **TELEMÁTICA**, a través de la Sede Electrónica, la plataforma de autogestión Tu Seguridad Social, Registro Electrónico, diversos servicios de intermediación e interconexión, la página web, el Buzón de Consultas y la aplicación móvil.

El presupuesto de gastos de la Entidad en transferencias corrientes por pago de prestaciones a los sujetos protegidos por el Sistema de Seguridad Social, asciende para el año 2020 a **131.580.672.970 EUROS**, prácticamente un tercio del presupuesto total nacional.

A finales de julio de 2020 había más de **17.600.000 TRABAJADORES** protegidos por la prestación de incapacidad temporal y se encontraban en vigor más de **9.700.000 PENSIONES** reconocidas y gestionadas por la entidad.

[LA MISIÓN DEL INSS ES GESTIONAR Y ADMINISTRAR LAS PRESTACIONES ECONÓMICAS DEL SISTEMA DE LA SEGURIDAD SOCIAL, DE ACUERDO CON LA LEGISLACIÓN NACIONAL E INTERNACIONAL EN LA MATERIA, CON EXCEPCIÓN DE AQUELLAS CUYA GESTIÓN ESTÁ ATRIBUIDA AL INSTITUTO SOCIAL DE LA MARINA [ISM], AL SERVICIO PÚBLICO DE EMPLEO ESTATAL [SPEE], AL INSTITUTO DE MAYORES Y SERVICIOS SOCIALES [IMSERSO] O A LOS SERVICIOS COMPETENTES DE LAS COMUNIDADES AUTÓNOMAS].

En datos anuales, tomando como referencia el año **2019**, cabe destacar las siguientes magnitudes:

- >> **7.442.353** Clientes atendidos presencialmente
- >> **1.020.883** Consultas telefónicas atendidas
- >> **61.908** Consultas telemáticas formuladas
- >> **1.170.468** Trámites por Registro Electrónico
- >> **10.379** Empleados a 31 de diciembre 2019

[VISIÓN: EL INSS QUIERE SER PERCIBIDO COMO UNA ORGANIZACIÓN DE REFERENCIA, QUE SATISFACE LAS EXPECTATIVAS DE LOS CIUDADANOS Y OBTIENE AL MISMO TIEMPO LA MEJOR VALORACIÓN SOCIAL Y ECONÓMICA. PARA ELLO APOYAMOS NUESTRA ACTUACIÓN EN VALORES COMO LA ORIENTACIÓN AL CLIENTE, LA ORIENTACIÓN A LOS RESULTADOS, LA AGILIDAD, LA CREATIVIDAD, LA FLEXIBILIDAD Y LA VOCACIÓN DE SERVICIO.

COMO ORGANIZACIÓN PÚBLICA EL INSS ESTÁ COMPROMETIDO CON LA MEJORA CONTINUA DE SUS PROCESOS Y SERVICIOS PARA LO CUAL FOMENTA LA PARTICIPACIÓN DE LOS CIUDADANOS Y LA TRANSPARENCIA, COMO ELEMENTOS FUNDAMENTALES DE ACTUACIÓN]

COMPROMISO CON LA CONFIDENCIALIDAD: LA CARTA DE SERVICIOS DEL INSS

<< EL DERECHO A LA PROTECCIÓN DE SUS DATOS PERSONALES, Y EN PARTICULAR EL DERECHO A LA SEGURIDAD Y CONFIDENCIALIDAD DE LOS DATOS QUE FIGUREN EN LOS FICHEROS, SISTEMAS Y APLICACIONES DEL INSS >>

CUADRO 3

Como ejemplo de este compromiso, en la Carta de Servicios para el período 2019-2021 se explicita, entre los **DERECHOS CONCRETOS DE LOS CIUDADANOS Y USUARIOS EN RELACIÓN CON LOS SERVICIOS** una mención específica a la protección de datos y la confidencialidad, como se destaca en el **CUADRO 3**.

El volumen y diversidad de interacciones que realiza nuestra Entidad con los ciudadanos cada año **[CUADRO 4]** da fundamento y refuerza el compromiso de la organización con la privacidad.

VOLUMEN DE INTERACCIONES Y ACTOS INFORMATIVOS CON LOS CIUDADANOS

7.442.353 CONSULTAS ATENDIDAS EN OFICINA

1.020.883 CONSULTAS ATENDIDAS POR TELÉFONO

61.908 CONSULTAS TELEMÁTICAS ATENDIDAS

1.170.468 TRÁMITES POR REGISTRO ELECTRÓNICO

FILOSOFÍA QUE HA GUIADO EL PROCESO DE ADAPTACIÓN

Dentro del complejo contexto descrito, la adaptación al nuevo RGPD ha supuesto un gran **RETO** para nuestra Entidad, ya que no se trataba de una modificación normativa al uso sino de un verdadero cambio de filosofía que suponía un **GIRO DE 180º**, desde un esquema estandarizado y rígido basado en la verificación del cumplimiento de una bateria de medidas preestablecidas con independencia de las circunstancias de la organización, con un enfoque pasivo y reactivo; hacia otro flexible y en permanente adaptación para responder a las nuevas necesidades propias de la *modernidad líquida*, como la describía Bauman, y de un universo digital en constante y vertiginosa evolución.

Un nuevo esquema **MÁS EXIGENTE** a efectos de su aplicación efectiva en las organizaciones y que supone un considerable incremento de la responsabilidad, respecto al esquema anterior, al fundamentarse en el análisis, ponderación y ajuste permanente a un entorno cambiante, y apoyarse en dos conceptos clave: **LA PROACTIVIDAD Y LA DILIGENCIA**, aspectos poco habituales hasta la fecha en nuestra legislación.

De forma simultánea, también ha supuesto una gran **OPORTUNIDAD** para revisar, reorganizar, estructurar, racionalizar y mejorar todos nuestros procesos y la estructura que les da soporte desde la perspectiva de la protección de los datos personales, la seguridad de la información y del refuerzo de las garantías de los derechos y libertades de los ciudadanos en esta materia.

De esta forma, el nuevo RGPD ha sido el **IMPULSO** necesario para acometer una labor titánica de revisión y cambio de enfoque, con una batería de todo tipo de medidas que afectan a todos los ámbitos de gestión para dar cumplimiento a la norma, imbuir de su espíritu a todos los estamentos de la Entidad e implicar a toda la organización en ese propósito.

La filosofía aplicada a esta adaptación se ha apoyado fundamentalmente en:

- Tres **PILARES**: experiencia, implicación y racionalización, que han sido la base sobre la que se ha construido nuestro nuevo modelo de privacidad.
- Tres **VALORES**: homogeneidad, eficiencia y agilidad que han orientado nuestra actuación.
- Una consolidada dinámica de ciclos de análisis, enfoque, desarrollo y mejora continua ampliamente consolidados fruto de nuestra experiencia en la aplicación del **MODELO EFQM DE EXCELENCIA**.
- Seis **PRINCIPIOS INSPIRADORES** que han guiado el análisis y la toma de decisiones, según se plasma en el diagrama siguiente **[CUADRO 5]**.

FACTORES CLAVE EN EL PROCESO DE ADAPTACIÓN

CUADRO 5

>> RACIONALIZACIÓN

Gracias a la experiencia atesorada, al enfoque práctico-pragmático y el **ENFOQUE DUAL** (centralizado/descentralizado) adoptados, se ha podido acometer, en un breve plazo de tiempo, una profunda revisión de todos y cada uno de nuestros procesos con impacto en protección de datos (comenzando por aquellos procesos principales para ir descendiendo y profundizando progresivamente hacia procesos secundarios o especializados).

Esto ha supuesto que, basándonos en el aprendizaje y experiencia acumulada, a través de situaciones que previamente habíamos identificado como susceptibles de mejora y del seguimiento de los resultados más y menos satisfactorios de actuaciones e iniciativas anteriores, tanto propias como ajenas, hayamos podido racionalizar, de forma ágil, exitosa y con buenos resultados, muchos de nuestros procesos.

Para ello hemos aplicado técnicas propias de la gestión de la calidad y el enfoque de la excelencia (según el modelo EFQM seguido por nuestra organización), la gestión por objetivos y por procesos o la planificación estratégica. Priorizando siempre valores esenciales durante todo el proceso, como son la agilidad y la eficiencia.

Uno de los ejemplos más significativos para ilustrar lo anterior, es el que afecta al **REGISTRO DE ACTIVIDADES DE TRATAMIENTO (RAT) (ANEXO 1)** y, en consecuencia, al **INVENTARIO DE ACTIVIDADES DE TRATAMIENTO** (IAT) publicado en nuestra página web (www.seg-social.es).

En este caso, como se muestra en el **CUADRO 6,** se ha pasado de:

- Gestionar el registro y actualización de más de 1450 ficheros
- distribuidos por todo el territorio nacional,
- determinados según un criterio algo dispar y lastrado por una consideración limitada del concepto de fichero,

a un registro con 43 tratamientos (o macrotratamientos coincidentes con los procesos fundamentales de la gestión del INSS, **[CUADRO 20]** aplicando la filosofía de la reingeniería radical de procesos tras verificar que el esquema de que se disponía no daba respuesta a las necesidades de la Entidad, ni desde el punto de vista organizativo y de la gestión ni desde el más relevante, desde la perspectiva de la mejor garantía de la protección de los derechos y libertades de los ciudadanos en el ámbito de la privacidad.

De tal forma que se comprobó que el esquema no cumplía con un criterio de **HOMOGENEIDAD**, necesario en una organización, que aunque ampliamente descentralizada, ejerce su actividad con unidad de acción en todo el ámbito estatal.

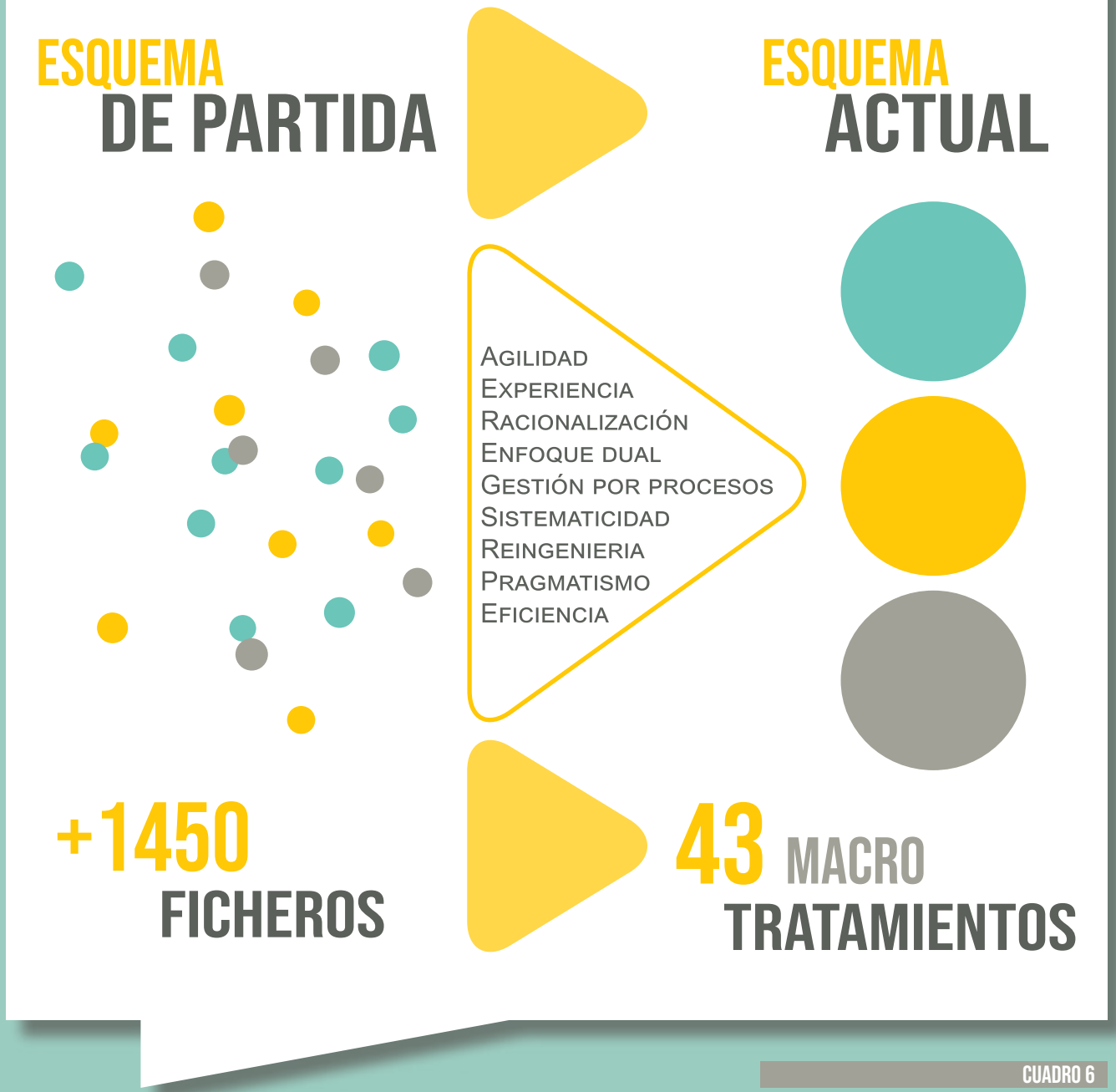
Tampoco respondía a las necesidades de mantenimiento y actualización en momentos en los que la organización debe centrar más que nunca sus esfuerzos en un uso eficiente de sus limitados recursos.

La **ATOMIZACIÓN Y MULTIPLICACIÓN DE FICHEROS** también se comprobó que no representaba ninguna ventaja desde el punto de vista de la protección de los datos pues, por una parte se descendía al detalle de microoperaciones y tareas englobadas en los procesos ordinarios de la gestión, pero por otra no se prestaba atención a aquellas otras operaciones y tareas que, aunque se realizaban con carácter habitual en todos los puntos de la organización, no se realizaban a través de una aplicación informática ni se apoyaban en bases de datos tradicionales, con lo que se obviaba su declaración y existencia, con independencia de lo relevante del tratamiento o de la sensibilidad de los datos personales a los que afectaba, y por tanto, no eran objeto de aplicación y revisión al mismo nivel que las registradas.

Así que, basándonos en la experiencia acumulada, se tomó una **DECISIÓN PROACTIVA** que huía del conformismo, desechando la idea de crear el Registro de Actividades de Tratamiento como una mera traslación del antiguo esquema de ficheros al de tratamientos, mediante la equiparación directa de unos a otros. Ya que, aunque suponía un costoso proceso de análisis y racionalización era un **ESFUERZO NECESARIO** en aras de:

- representar nuestro **COMPROMISO** con la privacidad,
- cimentar una **ESTRUCTURA SÓLIDA** que le daría soporte a esta nueva etapa, y
- dar paso decidido para hacer realidad una transformación de la filosofía de protección de datos de la organización hacia un **ENFOQUE 360º COMPROMETIDO, EFECTIVO Y REAL.**

RACIONALIZACIÓN COMO UN VALOR DE LA TRANSFORMACIÓN DE NUESTRO ESQUEMA DE PRIVACIDAD



CUADRO 6

>> EXPERIENCIA

La experancia acumulada durante una década de andadura en la vigilancia de la aplicación de la normativa de protección de datos personales por parte de la Inspección de Servicios del INSS a través de:

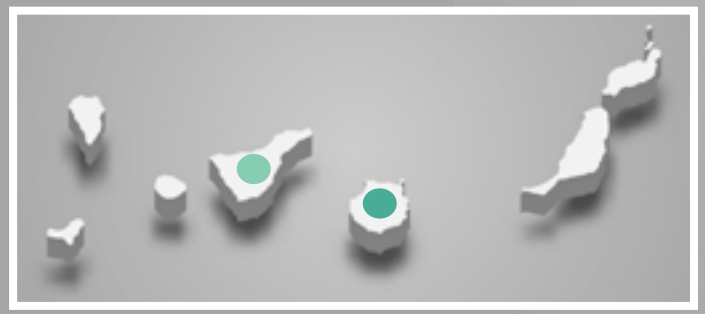
- un consolidado programa de inspección de protección de datos **(CUADRO 8)**
- la resolución de consultas formuladas por parte de las distintas unidades y
- la gestión de peticiones de ejercicio de derechos ARCO
- el control centralizado de la realización de las auditorías de protección de datos en todo el territorio nacional

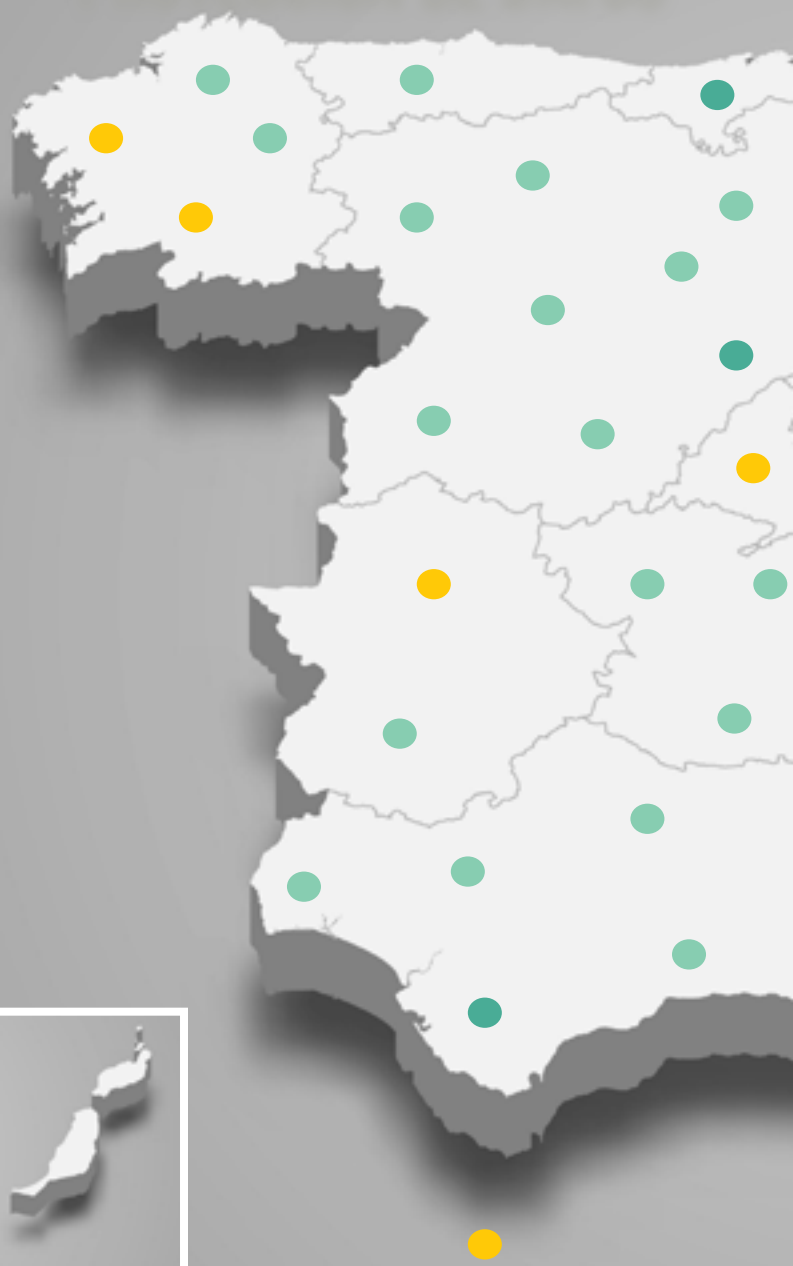
ha sido muy valiosa y ha constituido una sólida base en la que se ha apoyado todo el proceso de adaptación.

Durante este período, se profundizó en el conocimiento teórico-jurídico de la materia, sin duda necesario, pero también en su enfoque más práctico: al permitir comprobar la efectividad real y vicisitudes en su aplicación en los procesos de nuestra Entidad, así como conocer de primera mano su impacto real en nuestra gestión (tiempos de resolución, recursos necesarios para su implantación, …).

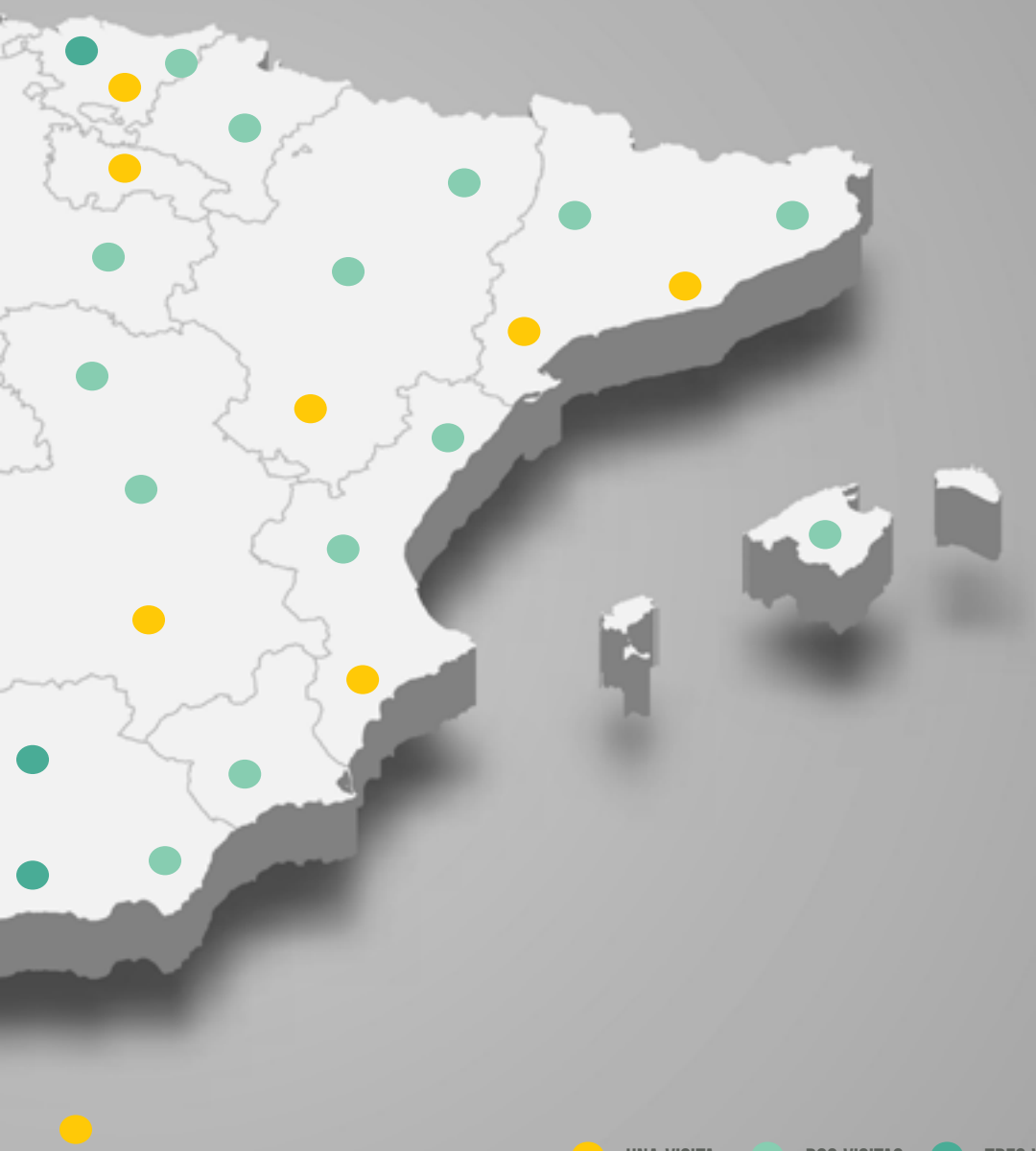
Esta experiencia ha aportado un interesante enfoque técnico-jurídico a la par que práctico, que ha orientado el proceso de adaptación de nuestros procesos y organización al nuevo Reglamento.

Todo ello, sin dejar de tener en cuenta algo crucial: el impacto de estas decisiones en la compleja gestión que tiene encomendada nuestro Instituto. En momentos en los que existe un importante déficit de recursos personales y en los que, además, se están acometiendo profundas y relevantes modificaciones normativas en Seguridad Social y en otros ámbitos, como el procedimiento administrativo y la Administración Electrónica, que obligan a compatibilizar el avance en la adaptación normativa en todos esos campos y el cumplimiento con los plazos legales establecidos para su implantación, sin por ello menoscabar la gestión de las prestaciones de Seguridad Social, razón de la existencia de esta Entidad.





EL PROGRAMA DE



UNA VISITA DOS VISITAS TRES VISITAS

CUADRO 7

CONTENIDO DEL PROGRAMA DE INSPECCIÓN DE PROTECCIÓN DE DATOS PERSONALES

1.ENTORNO FUNCIONAL Y HUMANO

1.1.- Organigrama de la Dirección Provincial.
1.2.- Idoneidad de la plantilla y especialización en materia de protección de datos. Existencia de responsables encargados de supervisar el cumplimiento de la normativa de protección de datos por parte del personal de la DP.

2.ENTORNO FÍSICO Y TECNOLÓGICO

2.1.- Equipamiento material y equipamiento informático.
2.2.- Sistemas de información y aplicativos informáticos. Verificación de tratamientos y registro.

3. ENTORNO PROCEDIMENTAL

3.1.- Consentimiento del afectado.
3.2.- Acceso a los datos personales por personal externo, contratos y cláusulas de confidencialidad.
3.3.- Cesión y Transferencia Internacional de datos.
3.4.- Registro de actividades de tratamientos de datos.
3.5.- Responsable/s y Encargados del tratamiento de datos.
3.6.- Alta usuarios SILCON: administradores, usuarios, nivel de autorización, adecuación de las autorizaciones a las funciones desempeñadas, formación específica en protección de datos.
3.7.- Medidas de seguridad de los tratamientos automatizados y no automatizados.
3.8.- Auditorías.
3.9.- SARTIDO. Administrador, usuarios y adecuación de los permisos a las funciones, proporción en relación a la plantilla y distribución por áreas funcionales, carpeta documentación médica y carpeta de documentación sensible.
3.10.- Copias de respaldo y recuperación.
3.11.- Reconocimientos médicos de empleados. Responsables internos / externos, conservación de documentación con datos sensibles.
3.12.- Acción social y expedientes del personal.
3.13.- Destrucción de documentación: expurgo.
3.14.- Actuaciones y formación del personal en materia de protección de datos.
3.15.- Protocolo ejercicio derechos ARCO y otros.
3.16.- Unidades médicas de evaluación y valoración de incapacidad (UMEVI). Medidas de seguridad, gestión de los procedimientos de identificación y llamamiento de los usuarios, documentación médica, , autorizaciones para el acceso al historial médico, sesiones EVI, aplicativos informáticos.
3.17.- Videovigilancia.

4. OTROS ASPECTOS A CONSIDERAR

4.1.- Transparencia y Acceso a la Información Pública.
4.2.- Buzón de Opinión y Quejas y Sugerencias.

CUADRO 8

>> IMPLICACIÓN

Entendemos que para una efectiva protección de los datos personales es necesaria la implicación de todas las personas de la organización e, incluso, de aquellas otras que, sin formar parte de ésta, interaccionan con ella a través de la prestación de servicios en nuestras instalaciones o fuera de ellas, o mediante la puesta a disposición de acceso a sus bases de datos o que tienen acceso a las nuestras.

De esta forma, siendo conscientes de las grandes dificultades que supone llegar a todas las personas de dentro y fuera de la organización con acceso habitual o puntual a datos personales, se ha optado por un doble enfoque que combina la centralización y la descentralización en función del objetivo perseguido:

- Por una parte, de **CENTRALIZACIÓN**, para asegurar la homogeneidad, coherencia y unidad de acción así como la eficiencia de los procesos, y
- Por otra, de **DESCENTRALIZACIÓN**, para ampliar la eficacia de las medidas tomadas y que éstas lleguen a todos los puntos de la organización,

También se ha aplicado este enfoque para incrementar y mejorar la capacidad de detección y análisis de riesgos y oportunidades.

De esta forma, este **PATRÓN DUAL** se concreta en:

- **DESCENTRALIZACIÓN** en la responsabilidad de aplicar tanto las medidas y criterios adoptados como de efectuar la vigilancia más cercana de su cumplimiento todo ello articulado a través de una red de contactos con representación en cada una de las provincias del ámbito nacional, para maximizar así nuestra capacidad de actuación y control en todo el territorio.
- **CENTRALIZACIÓN** de la toma de decisiones, resolución de consultas y peticiones, la canalización de las comunicaciones y elevación de propuestas al DPD (SPD y equipo de apoyo) y de todo lo concerniente a la comunicación interna e institucional sobre esta materia, como la edición de materiales y gestión de contenidos en la Intranet y en la web, entre otros.

Así como, del control y vigilancia del cumplimiento de las instrucciones impartidas a través del programa de Inspección y del correcto desarrollo del plan de auditorías.

- **DESCENTRALIZACIÓN**, así mismo, en la identificación de focos de riesgo de protección de datos y de rastreo de oportunidades de adaptación, revisión y mejora de procesos internos, aplicaciones y documentos, desde la perspectiva de la protección de datos (grupo de trabajo de protección de datos con representantes de todas las Subdirecciones Generales y comunicaciones recogidas a través de la red de responsables de protección de datos en el ámbito provincial).

>> HOMOGENEIDAD

Como consecuencia de la experiencia adquirida en la última década, hemos confirmado el valor crucial que constituye la homogeneidad de criterio y unidad de acción. Esto es clave en una organización ampliamente descentralizada para evitar que se pueda imponer la disparidad de actuación y proliferen distintas interpretaciones y enfoques en las actuaciones con impacto en la protección de datos personales.

Por ello, todas las actuaciones e iniciativas que se han llevado a cabo en este proceso de adaptación han tenido como hilo conductor la **COORDINACIÓN Y LA CENTRALIZACIÓN** de todas aquellas cuestiones que se consideran estratégicas, mientras que se ha optado por la descentralización en su aplicación operativa, pero siempre bajo las directrices del SPD y su equipo de apoyo, con el refuerzo de otros instrumentos para asegurar su cumplimiento como son: los objetivos institucionales, el plan de auditorías y las inspecciones de servicio presenciales o ahora telemáticas. De esta forma se asegura la capacidad de actuar sobre un amplio territorio y una numerosa plantilla así como la eficacia de las medidas aplicadas, sin por ello menoscabar la unidad de criterio y la homogeneidad en nuestra actuación.

>> AGILIDAD

Otra de las preocupaciones a la hora de diseñar las medidas necesarias para la adaptación al RGPD ha sido el que ésta sea ágil sin por ello renunciar al rigor jurídico ni a las máximas garantías técnicas, ponderando en todo caso los recursos disponibles, el enfoque del riesgo y el impacto en la gestión de las prestaciones del sistema de Seguridad Social.

En este sentido, en algunos supuestos se ha tomado la determinación de acometer **MEDIDAS DE EXIGENCIA INCREMENTAL**, priorizando aquellas cuestiones que tenían mayor impacto en los derechos y garantías de los ciudadanos, para luego ir desarrollando las medidas aplicadas, en fases sucesivas, ampliando, reforzando y, en su caso, elevando el nivel de exigencia de las garantías que ofrecen.

De esta forma se consigue una primera actuación ágil que asegura una cobertura básica en todos los focos de interés en materia de protección de datos, en un periodo de tiempo reducido y, posteriormente, a través de **CICLOS DE ITERACIONES** se desarrollan para incrementar su efectividad y radio de acción.

De forma simultánea, en estos procesos reiterativos se revisan y evalúan los resultados obtenidos, las incidencias que han surgido en ese proceso y se detectan nuevos riesgos y áreas de mejora sobre las que actuar y se implementan las mejoras y actualizaciones necesarias. Incidiendo positivamente en el proceso de aprendizaje y adquisición de **EXPERIENCIA** que refuerzan la eficacia de nuestra actuación.

>> EFICIENCIA

El tercer valor fundamental de este proceso ha sido la eficiencia. En el difícil contexto planteado es crucial invertir todos nuestros esfuerzos en que los procesos y actuaciones se diseñen bajo el prisma de la eficiencia y la promuevan en todos los ámbitos. Además de las obvias ventajas de este enfoque hay que añadir una relacionada con la motivación e implicación de todos los actores que intervienen en la puesta en marcha de esta adaptación.

Esto es así porque hay que admitir que la protección de datos, durante mucho tiempo ha sido percibida como una sobrecarga para la gestión propia de las organizaciones, seguramente por un **ENFOQUE BUROCRÁTICO** en su aplicación y un planteamiento mejorable en la concienciación y comunicación tanto de las medidas de seguridad como del resto de obligaciones que implicaba esta normativa, por lo que no se consiguió una plena interiorización por parte de todos aquellos que tenían que tenerla en cuenta a la hora de ejercer su actividad.

Por ello, asumiendo esa situación de partida, era necesario que los actores implicados percibieran que esta adaptación no iba a suponerles una carga adicional de trabajo, como en ocasiones anteriores, sino que iba a ser aprovechado por la Entidad como una oportunidad para **ELIMINAR CARGAS BUROCRÁTICAS** que nada aportaban a la efectiva protección de los datos personales y para centralizar todo aquello que hasta el momento se venía haciendo de forma repetida y repartida por todo el territorio, consumiendo muchos recursos, cuando en realidad podía realizarse una única vez a nivel centralizado, liberando los limitados recursos de que disponen. Esta estrategia ha sido muy bien acogida y ha coadyuvado también a otro de los valores ya mencionados, la **HOMOGENEIDAD**.

RUTA PARA EL CUMPLIMIENTO Y ADAPTACIÓN

EL CAMINO SEGUIDO PARA LLEVAR A CABO LA ADAPTACIÓN DE NUESTRA ORGANIZACIÓN A LOS NUEVOS REQUERIMIENTOS Y EXIGENCIAS DEL RGPD HA SUPUESTO LA SUPERACIÓN DE DISTINTAS FASES SUCESIVAS O SIMULTÁNEAS, SI BIEN, ESTE PROCESO DE ADAPTACIÓN NUNCA TERMINA Y ESTÁ EN PERMANENTE REVISIÓN. A CONTINUACIÓN SE DESTACAN LAS ACTUACIONES MÁS RELEVANTES E ILUSTRATIVAS DEL PROCESO SEGUIDO QUE SE ENGLOBAN EN CADA UNA DE ELLAS.

FASE EXPERIENCIA

Esta fase comprende todas las actuaciones realizadas hasta la aprobación del RGPD y que han servido de base para:

- atesorar el conocimiento teórico-jurídico y práctico,
- conocer nuestras debilidades y fortalezas en esta materia
- saber identificar tanto los puntos fuertes como las áreas de mejora en materia de protección de datos en nuestros procesos y en la aplicación real y efectiva de medidas a nivel de toda la organización,
- predecir de manera fiable el impacto real que puede tener cada medida implantada en todos los ámbitos de la gestión
- y, en suma, mejorar nuestra capacidad organizacional de análisis, desde una **PERSPECTIVA 360°**.

Dentro de esta etapa, destacan:

Por su especial relevancia, y como fuente indispensable de conocimiento práctico y herramienta de homogeneización y concienciación, las **84 VISITAS DE INSPECCIÓN** realizadas en el programa de protección de datos, desde 2010 hasta el año 2017, con cobertura de todo el territorio nacional, a resultas de las que se han emitido:

- 440 instrucciones de obligado cumplimiento
- 239 propuestas de mejora

La creación de la **UNIDAD NACIONAL DE AUDITORÍAS DEL INSS**, responsable de la coordinación y control de los procesos de adecuación a la normativa de protección de datos y de realización de las auditorías bienales de los ficheros LOPD de la entidad, así como del control de la idoneidad de los accesos a los datos personales **[CUADRO 10]**.

ADECUACIÓN Y AUDITORÍA DE FICHEROS LOPD

En cumplimiento de las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre, se llevaron a cabo, periódicamente, planes de adecuación con el objetivo de que la Entidad cumpliera con la legislación de protección de datos, y -en colaboración con la Gerencia de Informática de la Seguridad Social (GISS)- auditorías bienales de los ficheros que contienen datos de carácter personal con exigencia de nivel de seguridad medio y alto. *[Ver* **ANEXO 2** *donde se recogen los cuestionarios de adecuación y auditoría general y el modelo de informe de Auditoría provincial remitidos a las DDPP para el desarrollo de esta actividad].*

NORMATIVO AL RGPD

AUDITORÍAS DE CONTROL DE ACCESOS:

Se efectúan las siguientes auditorías periódicas:

AUDITORÍA DE ACCESOS A TRAVÉS DEL SISTEMA DE CONFIDENCIALIDAD SILCON.

Mediante la Circular de este Instituto Num. 6/97, de 16 de octubre, sobre control y seguimiento de accesos a los ficheros automatizados del Instituto Nacional de la Seguridad Social a través del sistema de confidencialidad (SILCON), se estableció que se vigilaría el estricto uso de las autorizaciones de acceso otorgadas, adoptando las medidas correctoras oportunas y exigiendo las responsabilidades pertinentes. Asimismo, se estableció que con una periodicidad no superior a un mes se procedería a la revisión y análisis de los datos de la auditoría proporcionados por el sistema a través de las transacciones de auditoría. Con posterioridad, la Circular 2/2010, actualizó en ciertos aspectos la anterior.

CUADRO 9

AUDITORÍAS PROS@:

A través de las que se controla que los accesos de los empleados públicos del INSS a las aplicaciones del entorno informático PROS@ se adecúen a lo establecido

AUDITORÍAS IFI-WEB:

Esta auditoría se lleva a cabo de forma descentralizada desde las DDPP del INSS por parte de los auditores provinciales, respecto de los accesos realizados por organismos externos en cada provincia a los servicios de intercambio de ficheros institucionales de los que dispone el INSS (IFIWEB) a los que acceden a través de la página Web.

AUDITORÍAS PLATAFORMA DE INTERMEDIACIÓN

A través de las que se controla la corrección de los accesos realizados por organismos externos a los datos que el INSS pone a su disposición a través de la plataforma.

AUDITORÍAS DE ACCESOS A SERVICIOS EXTERNOS

La Unidad Nacional de Auditorías, asimismo, coordina las actuaciones necesarias para atender los requerimientos de organismos ajenos, como el Instituto Nacional de Estadística (INE), en las auditorías que efectúa respecto de los accesos efectuados por el INSS al Servicio de Verificación de Datos de Residencia (SVDR) o la Policía Nacional, en relación con los accesos al Servicio de Verificación de datos de Identidad (SVDI). [ANEXO 3. MODELO DE INFORME DE AUDITORÍAS]

LA IMPLANTACIÓN DE CICLOS DE OBJETIVOS INSTITUCIONALES CON IMPACTO EN PROTECCIÓN DE DATOS.

Desde el año 2013, el INSS, de acuerdo con su planificación estratégica, ha establecido objetivos provinciales en materia de protección de datos, cuyo grado de cumplimiento se valora semestralmente y se refleja en el nivel de productividad alcanzado:

>> INFORMES SOBRE AUDITORÍAS INFORMÁTICAS (2013-2018):

Persigue garantizar la adecuación de los accesos realizados a los datos incluidos en los sistemas de información. Se establece como objetivo que las DDPP auditen el 100% de los accesos cargados por la GISS en las transacciones de auditorías.

>> ADECUACIÓN INSTITUCIONAL A LA LOPD (2013-2018):

Persigue salvaguardar la protección de los datos personales a través del control de la realización de auditorías bienales a los ficheros con nivel de seguridad medio y alto. Se establece como objetivo que las DDPP auditen los ficheros respecto de los que venza en el semestre el periodo de dos años desde la auditoría anterior.

RR POLÍTICA DE USO SEGURO DE LOS SISTEMAS DE INFORMACIÓN DE LA SEGURIDAD SOCIAL (2015):

Establece como objetivo la realización por las DDPP de una acción de comunicación dirigida a todo su personal, con la finalidad de informar del contenido de las normas" Política de uso seguro de los sistemas de información de la Seguridad Social" y "Revisión del uso de los sistemas de información y tratamiento de evidencias electrónicas", adoptadas por el Comité de Seguridad de los Sistemas de Información de la Seguridad Social, y del "Curso de concienciación" disponible en la Intranet.

>> POLÍTICA DE USO SEGURO DE LOS SISTEMAS DE INFORMACIÓN DE LA SEGURIDAD SOCIAL (2016):

Persigue garantizar el uso seguro de los sistemas de información de la Seguridad Social. Para ello se impone a las DDPP, habilitar un espacio específico en la INTRANET provincial, destinado a la Política de uso seguro de los sistemas de información de la Seguridad Social, así como elaborar un cuadro–resumen de los derechos y obligaciones de los usuarios, y de los usos no permitidos. Deben, así mismo, difundir la novedad.

>> CONCIENCIACIÓN DIRIGIDA A LOS EMPLEADOS DEL INSS SOBRE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL (2017).

El objetivo persigue sensibilizar y recordar a los empleados de la Entidad las prescripciones de la LOPD. Para ello, las DDPP deben publicar una novedad mensual en la Intranet provincial, referida a los derechos y obligaciones de los usuarios de la Seguridad Social en materia de protección de datos de carácter personal. Deben, así mismo, difundir la novedad.

GESTIÓN DE LA INSCRIPCIÓN, MODIFICACIÓN Y SUPRESIÓN DE FICHEROS MEDIANTE EL APLICATIVO SIGLA

También debe mencionarse la gestión de la inscripción, modificación y supresión de ficheros mediante el aplicativo SIGLA. Así, de acuerdo con la legislación anterior, la Entidad llevó a cabo una importante tarea de identificación y análisis de los conjuntos organizados de datos personales estructurados en forma de ficheros, y de las medidas de seguridad exigibles, para su adecuada inscripción y mantenimiento en el Registro de ficheros de la AEPD.

LA TRAMITACIÓN DE DENUNCIAS, RESOLUCIÓN DE CONSULTAS E IMPARTICIÓN DE INSTRUCCIONES EN ESTA MATERIA.

Entre los años 2010 y 2018 se han tramitado 71 **EXPEDIENTES** relacionados con denuncias por accesos indebidos a datos personales, 5 expedientes sobre cesión, y se han atendido numerosas consultas sobre protección de datos personales. Paralelamente, en distintos momentos, se han emitido instrucciones sobre esta materia.

LA GESTIÓN DE PETICIONES Y EJERCICIO DE DERECHOS ARCO.

En cumplimiento de las previsiones de la anterior legislación de Protección de Datos, el INSS, a través de la Secretaría General a nivel Central, y de las DDPP, en el ámbito periférico, ha venido atendiendo las solicitudes de los interesados, en relación con sus datos de carácter personal, y facilitando a estos el ejercicio de los derechos de acceso, rectificación, cancelación y oposición reconocidos por la normativa.

Así, en satisfacción del derecho de acceso se proporcionaba a los interesados la información, recabada de las Subdirecciones Generales responsables de los distintos ficheros y sistemas de información, respecto de sus concretos datos personales obrantes en poder de la entidad, finalidad para la que fueron recabados, periodo de conservación de los mismos, cesiones, en su caso, previstas, y autoridad de control ante la que formular reclamaciones en esta materia.

LA COLABORACIÓN INSPECTORA EN LOS EXPEDIENTES DISCIPLINARIOS POR VULNERACIÓN DE LA PROTECCIÓN DE DATOS.

La Inspección de Servicios de la Entidad da traslado a la Subdirección General de Recursos Humanos y Materiales, unidad competente para la instrucción de los expedientes disciplinarios, de todos aquellos supuestos en los que se detectan indicios de actuación irregular del personal del Instituto, en relación con la protección de los datos personales de los ciudadanos y del resto de los funcionarios o personal laboral.

Para ello, en los casos en que se recibe una **DENUNCIA** de acceso indebido a datos personales de un ciudadano o de cualquier empleado del INSS, se solicita de la Gerencia de Informática de la Seguridad Social (GISS) que realice una **ACTIVIDAD DE ANÁLISIS FORENSE DE ACCESO A DATOS** consistente en:

- una relación de los datos accedidos,
- junto con los códigos de identificación de los funcionarios que han llevado a cabo el acceso, en el período sobre el que se formula la denuncia o, de no concretarse éste, en el año anterior a la fecha de formulación de la misma.

Una vez obtenidos de la GISS los rastros solicitados, se pide al superior jerárquico del personal denunciado, un informe acerca de la idoneidad de los accesos - adecuación o correspondencia de los accesos con las funciones y competencias desempeñadas-. En caso de no quedar acreditada la correspondencia, se ponen los hechos en conocimiento de la Subdirección General de Recursos Humanos que, de considerarlo necesario solicita a la Inspección la realización de una información reservada (actuación inspectora de investigación), con carácter previo a la incoación del expediente disciplinario correspondiente.

De la misma manera, cuando el presunto acceso indebido se deduce de las **AUDITORÍAS** que realiza mensualmente la **UNIDAD NACIONAL DE AUDITORIAS**, se recaba informe del superior jerárquico del empleado cuyo resultado de auditoría no ha sido *a priori* favorable, y una vez se constata que se mantiene el criterio de que el acceso de que se trate ha sido indebido, se ponen los hechos en conocimiento de la citada Subdirección General, competente en esta materia.

Como resultado de lo anterior, desde 2010 se han tramitado en el INSS **18 EXPEDIENTES DISCIPLINARIOS** relacionados con accesos indebidos a datos personales, lo que representa un porcentaje mínimo en relación con el total de la plantilla de la Entidad.Concretamente un 0,18% de la plantilla en un periodo de 10 años y que, puesto en relación con el volumen de movimientos que se auditan, se traduce en una incidencia aislada y residual.

Ello es debido, sin duda, a una larga labor de divulgación, formación y otras actuaciones llevadas a cabo para conseguir la progresiva concienciación del personal sobre la importancia de preservar los datos personales y del cumplimiento más escrupuloso de la normativa de protección de datos. Sin olvidar, los efectos disuasorios del sistema de auditorías, conocido por todo el personal, y la rotundidad de las actuaciones disciplinarias que se derivan de los usos indebidos en caso de incumplimiento.

ACCIONES PARA LA CONCIENCIACIÓN EN MATERIA DE PROTECCIÓN DE DATOS (PD)

La elaboración de documentos divulgativos para la concienciación sobre PD de los trabajadores del Instituto. Entre la documentación que se entrega al personal que se incorpora a prestar servicios en el INSS, se han venido incluyendo folletos informativos en materia de protección de datos. **[CUADRO 22]**

FORMACIÓN Y CHARLAS

La formación y charlas impartidas (entre 2000 y 2018 se han impartido **175 EDICIONES** de cursos sobre la materia, con las siguientes denominaciones:

- “Protección de datos de carácter personal”
- “Atención al público y Protección de datos”
- "Ley Orgánica de Protección de Datos para empleados públicos”

con **3.802 ASISTENTES** en el conjunto de la Entidad.

VOLUMEN DE ACCESOS Y MEDIDAS DE CONTROL Y AUDITORÍA PARA GARANTIZAR LA PRIVACIDAD DE LOS DATOS EN EL INSS

95 VISITAS DE INSPECCIÓN DE PROTECCIÓN DATOS

PROGRAMA DE INSPECCIÓN CONSOLIDADO

458 INSTRUCCIONES

INSTRUCCIONES DE OBLIGADO CUMPLIMIENTO

261 PROPUESTAS DE MEJORA

INSTRUCCIONES DE OBLIGADO CUMPLIMIENTO

6 TIPOS DE AUDITORIAS INTERNAS Y EXTERNAS PERMANENTES

182 ORGANISMOS AUDITADOS

380 MIL ACCESOS AUDITADOS

654.252.081

ACCESOS A LAS PRINCIPALES BASES DE DATOS CORPORATIVAS EN 2019

4 BRECHAS DE SEGURIDAD NOTIFICADAS DESDE 2018

CUADRO 10

FASE

ANÁLISIS DEL IMPACTO DEL RGPD

A la vista de la publicación del RGPD, la Inspección de Servicios, a través de su personal especializado en protección de datos, realizó un análisis pormenorizado del impacto de esta modificación normativa en el ámbito de nuestra actividad y procedió a identificar las áreas de actuación y acciones necesarias para llevar a cabo esa adaptación de manera efectiva y exhaustiva.

En este análisis se aplicó, como venimos poniendo de manifiesto a lo largo de esta memoria, no sólo un **ENFOQUE JURÍDICO**, sino también **PRÁCTICO**, teniendo en cuenta:

- la situación de partida,
- los recursos disponibles, y
- la diversidad de casuística dentro de toda la red de centros de nuestra organización,
- así como las particularidades de las distintas áreas de especialización y ámbitos de competencia.

Como fruto de esa costosa labor, se publicó un informe titulado **"PRINCIPALES ASPECTOS A TENER EN CUENTA EN LA ADAPTACIÓN DE ESTE INSTITUTO AL NUEVO REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS" (ANEXO 4)**.

En él se abordan todas y cada una de las materias de nuestra esfera competencial que se ven afectadas por las modificaciones normativas y por el **CAMBIO DE FILOSOFÍA** en este ámbito. Siempre manteniendo el enfoque basado en la experiencia, a través de notas sobre la realidad práctica verificada en las actuaciones inspectoras con el fin de evitar situaciones y errores pasados. En estos apuntes se identifican y se llama la atención sobre áreas de mejora que deben abordarse y puntos débiles que necesitan reforzarse o corregirse en el proceso de adaptación.

El citado informe también recopila todas esas áreas en un listado que alcanza un total de **65 GRANDES CUESTIONES Y ACTUACIONES CONCRETAS IDENTIFICADAS** como actividades clave para la completa adaptación a la nueva normativa, teniendo en cuenta también el, entonces, proyecto de nueva LOPD.

Adicionalmente, en el documento se efectúa una **PRIORIZACIÓN** del listado de actuaciones, plasmado en un primer cronograma que figura como anexo al Informe. El resto de anexos hace referencia a aspectos importantes como:

- el modelo de doble capa para dar cumplimiento al deber de información;
- un modelo de contrato de encargo de tratamiento adaptado a la realidad de nuestra Entidad, tomando como base el publicado en la guía publicada por la AEPD sobre esta cuestión;
- o el informe-propuesta que se realizó desde nuestra Entidad sobre la figura del Delegado de Protección de Datos y las consideraciones sobre la forma de su configuración a nivel de la SESSP.

Este informe se **DIFUNDIÓ** entre los máximos responsables de la organización para su conocimiento y consideración. El documento recibió buenas valoraciones por su contenido y enfoque jurídico práctico centrado en la casuística real de la organización.

Para completar la **DIFUSIÓN Y CONOCIMIENTO,** se convocó a los 52 secretarios provinciales, muy vinculados con la aplicación de la norma en diversas áreas clave y representantes de los máximos responsables de cada dirección provincial, junto con otros responsables de las distintas áreas de los Servicios Centrales, en una jornada informativa en Madrid con el fin de explicar las cuestiones más importantes de ese informe tanto a nivel general como desde la perspectiva de su impacto en la esfera competencial provincial, además de aprovechar la ocasión para trasladar la nueva filosofía de la norma y el enfoque que el INSS había decidido tomar de cara a la necesidad de adaptación al nuevo Reglamento.

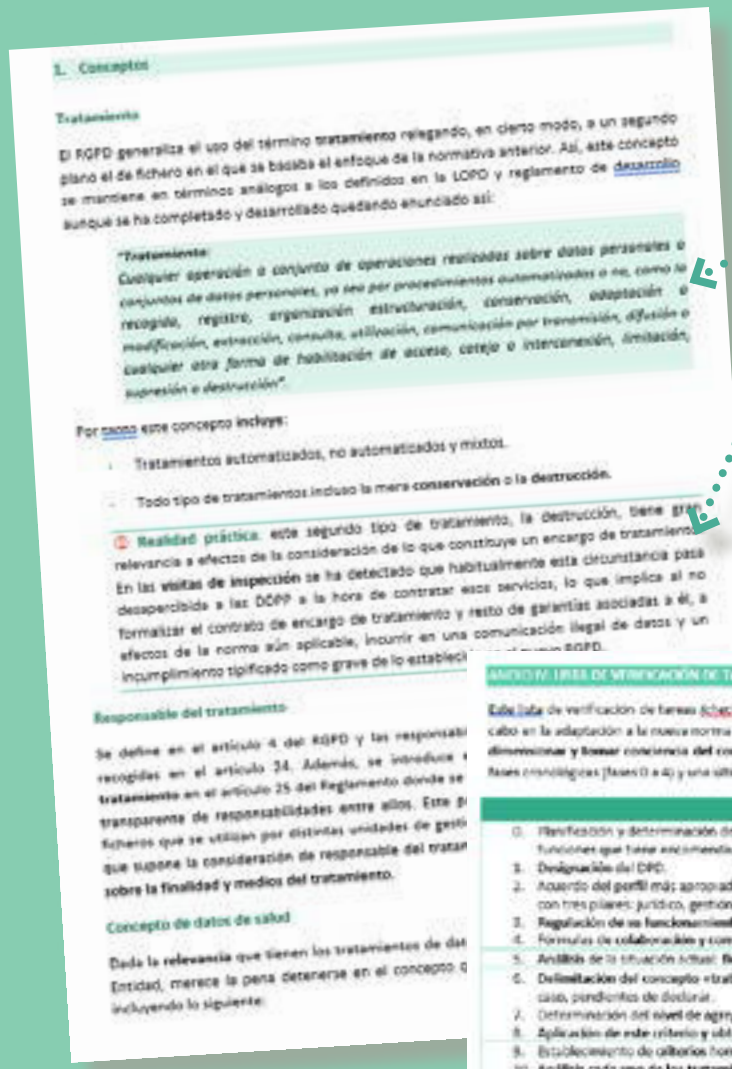
"PRINCIPALES ASPECTOS A TENER EN CUENTA EN LA ADAPTACIÓN DE ESTE INSTITUTO AL NUEVO RGPD"

DEFINICIONES

NOTAS DE "REALIDAD PRÁCTICA"

CONSECUENCIAS PARA LA GESTIÓN Y ACTUACIONES A REALIZAR

CRONOGRAMA DE ACTUACIONES



1. Conceptos

Tratamiento

El RGPD generaliza el uso del término **tratamiento** relegando, en cierto modo, a un segundo plano el de fichero en el que se basaba el enfoque de la normativa anterior. Así, este concepto se mantiene en términos análogos a los definidos en la LOPD y reglamento de desarrollo aunque se ha completado y desarrollado quedando enunciado así:

"**Tratamiento**:
Cualquier operación o conjunto de operaciones realizados sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

Por tanto este concepto **incluye**:

- Tratamientos automatizados, no automatizados y mixtos.
- Todo tipo de tratamientos incluso la mera **conservación** o la **destrucción**.

Realidad práctica: este segundo tipo de tratamiento, la destrucción, tiene gran relevancia a efectos de la consideración de lo que constituye un encargo de tratamiento. En las **visitas de inspección** se ha detectado que habitualmente esta circunstancia pasa desapercibida a las DOPP a la hora de contratar esos servicios, lo que implica al no formalizar el contrato de encargo de tratamiento y resto de garantías asociadas a él, a efectos de la norma aún aplicable, incurrir en una comunicación ilegal de datos y un incumplimiento tipificado como grave de lo estableci... el nuevo RGPD.

Responsable del tratamiento

Se define en el artículo 4 del RGPD y las responsabi... recogidas en el artículo 24. Además, se introduce ... **tratamiento** en el artículo 25 del Reglamento donde se ... transparente de responsabilidades entre ellos. Este p... ficheros que se utilizan por distintas unidades de gesti... que supone la consideración de responsable del tratam... **sobre la finalidad y medios del tratamiento**.

Concepto de datos de salud

Dada la **relevancia** que tienen los tratamientos de dat... Entidad, merece la pena detenerse en el concepto ... incluyendo lo siguiente:

ANEXO IV. LISTA DE VERIFICACIÓN DE TAREAS A REALIZAR Y CRONOGRAMA GENÉRICO POR ETAPAS PARA LA ADAPTACIÓN AL NUEVO REGLAMENTO

Esta lista de verificación de tareas (checklist) y cronograma genérico **no pretende ser una lista exhaustiva** de todas las actuaciones que deberían llevarse a cabo en la adaptación a la nueva norma pero sí que valga de guía en ese proceso y su orden cronológico de aplicación así como, en especial, **que sirva para dimensionar y tomar** conciencia **del considerable tiempo y recursos que habrá que dedicar** a ello en un tiempo muy limitado. Esta tabla se articula en 5 fases cronológicas (fases 0 a 4) y una última cecila (P) que hace referencia a aquellas tareas de carácter permanente.

ACCIONES	0	1	2	3	4	P
0. Planificación y determinación de la estructura y grado de participación de las entidades gestoras y servicios comunes en las funciones que tiene encomendadas la figura del **Delegado de protección de datos**.						
1. **Designación** del DPD.						
2. Acuerdo del perfil más apropiado para dar apoyo al DPO o SPD (valorar la propuesta de este informe respecto a una unidad con tres pilares: jurídico, gestión y experiencia técnico-práctica) y constitución de la unidad/es de apoyo.						
3. **Regulación de su funcionamiento**.						
4. Fórmulas de **colaboración y comunicación** entre unidades.						
5. **Análisis** de la situación actual: **Ficheros** declarados a nivel centralizado y descentralizado.						
6. **Delimitación del concepto «tratamiento»** a los efectos de la regularización y depuración de los ficheros declarados y, en su caso, pendientes de declarar.						
7. Determinación del **nivel de agregación/desagregación** (funcional y geográficas) que va a aplicarse.						
8. **Aplicación de este criterio y obtención de un listado de tratamientos.**						
9. Establecimiento de **criterios** homogéneos para la identificación de las **bases legales** para el tratamiento.						
10. **Análisis** caso **uno de los tratamientos** que realizamos para establecer dichas bases de legitimación.						
11. En caso de que la base de legitimación sea una **obligación legal, habrá de comprobarse**, si se confirma la redacción del PLOPD, que **ésta se deriva de una ley o norma de derecho de la UE.**						
12. **Análisis del alcance jurídico del Considerando 43.**						
13. **Estudio especial de los casos basados en el consentimiento**						
14. En su caso, estudio de aquellos **consentimientos** que **no cumplan con la nueva norma**, análisis de si puede ser sustituido con otra base jurídica.						
15. Cuando lo anterior no sea posible, **obtención de los nuevos consentimientos.**						
16. Determinar y desarrollar los mecanismos para **acreditar que se ha otorgado el consentimiento.**						

Deberá analizarse el **alcance jurídico** del Considerando 43 a efectos de nuestra consideración como «**autoridad pública**» y los efectos que de ésta se derivan respecto del uso del consentimiento como base legal legítima.

3. Transparencia e información a los interesados

El Considerando 58 y el artículo 12 de RGPD establecen las características que debe tener la **información otorgada a los interesados en virtud del principio de transparencia**:

- Concisa
- Transparente
- Inteligible
- De fácil acceso
- Lenguaje claro y sencillo

3.1 Consecuencias para nuestra gestión

La anterior implica que:

- La información deberá facilitarse por escrito o medios electrónicos, en su caso.
- Se evitará la remisión a textos legales. Por ej... siempre por **explicaciones accesibles para los interesados** con independencia de su nivel de conocimientos en la materia.
- La información que deberá facilitarse a los interesados se amplía, como se indica a ...

...rarse todas las comunicaciones y formatos que faciliten este ...cumplan con dichos requerimientos y serán, en todo caso, ...formato electrónico, en su caso.

...RGPD se aborda el deber de información en sus dos vertientes, ...obtenerse directamente del interesado o cuando se obtengan de ...fuentes ajenas.

...ar a los interesados recae sobre el responsable del ...

...ue a disposición de los interesados en el mismo momento ...y con carácter previo a su recogida o registro cuando ...

...ner en cuenta las definiciones del artículo 4 del RGPD en los ...sume que a efectos de este Reglamento el término «**autoridad**, ...cualquier organismo con potestades administrativas. La duda ...define el término «autoridad de control» como "**el delegado** ...cada miembro con arreglo a lo dispuesto en el artículo 51".

FASE NORMATIVA

Una vez realizado el análisis preliminar y culminada la planificación de las actuaciones a realizar, se comenzó con la fase normativa que dio estructura y soporte organizativo a la figura del **DELEGADO DE PROTECCIÓN DE DATOS**, subdelegados de protección de datos y a la Comisión formada por ellos.

Los artículos 37 a 39 del RGPD, y 34 y siguientes de la LOPDGDD, regulan la figura del DPD, que en el caso de nuestra entidad reviste carácter obligatorio. El RGPD prevé la posibilidad de designar un único DPD para varias autoridades u organismos cuando así parezca adecuado en atención a su estructura. En base a este precepto, el **CONSEJO GENERAL DE ADMINISTRACIÓN ELECTRÓNICA DE LA SEGURIDAD SOCIAL**, en su sesión de 31 de enero de 2017, adoptó el acuerdo de que exista un único DPD en el ámbito de la SESSP, designación que recayó en la persona titular de la Dirección del Servicio Jurídico de la Administración de la Seguridad Social.

Posteriormente, la Resolución de 17 de abril de 2018, de la SESSP **[VÉASE ANEXO 5],** reguló las funciones del DPD y creó la figura de los **SUBDELEGADOS DE PROTECCIÓN DE DATOS (SPD)**, en cada Entidad dependiente de la citada Secretaría de Estado, así como la **COMISIÓN DE PROTECCIÓN DE DATOS DE LA ADMINISTRACIÓN DE LA SEGURIDAD SOCIAL**, constituida por los SPD de cada Entidad, con funciones de apoyo al Delegado y contribución al cumplimiento de las previsiones en materia de protección de Datos.

El SPD del INSS es la persona titular de la Secretaría General, en la que, además concurre la competencia de coordinación de las Subdirecciones Generales de la Entidad, encomendada a esta unidad en las normas sobre estructura y competencias del INSS.

Consecuencia de su doble condición de SPD y Secretaria General de la Entidad, y en desarrollo de las competencias atribuidas por la mencionada Resolución de 17 de abril de 2018, de la Secretaría de Estado de la Seguridad Social, y Real Decreto 2583/1996, de 13 de diciembre, de estructura orgánica y funciones del INSS y de modificación parcial de la TGSS, cuyo artículo 6 le reconoce de forma expresa, entre otras, las facultades para la planificación estratégica y la promoción e implantación de procesos de mejora continua de la Entidad, ha venido a actualizar y dictar unas nuevas **INSTRUCCIONES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES**, de obligado cumplimiento para el conjunto de la Entidad y los empleados públicos adscritos a la misma **[VÉASE ANEXO 6]**.

Asimismo, se ha procedido a implementar las obligaciones derivadas de la interrelación entre la normativa de protección de datos personales y la contratación pública, y en especial las modificaciones operadas por el artículo 5 del Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, por el cual se ha modificado la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, en virtud de la cual pasa a ser contenido mínimo del contrato la referencia a la normativa de protección de datos, así como se establece la obligada inclusión en los pliegos de cláusulas administrativas particulares de

SEGURIDAD SOCIAL

INSS

INSTRUCCIONES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Instrucciones dictadas por la Secretaría General del INSS en su calidad de Subdelegada de Protección de Datos de la entidad para la adecuada implementación de la normativa de protección de datos personales en la gestión ordinaria de la actividad prestacional y del régimen interno del INSS.

PRIMERA	Digitalización y archivo electrónico de la documentación.
SEGUNDA	Bloqueo/Marcaje de expedientes.
TERCERA	Traslado y trasmisión de documentación a otros organismos.
CUARTA	Comunicaciones seguras.
QUINTA	Comunicaciones telefónicas.
SEXTA	Actividad contractual, cláusula de protección de datos.
SÉPTIMA	Bases de información y ficheros de datos.
OCTAVA	Sistemas de videovigilancia.
NOVENA	Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.
DÉCIMA	Identificación de los empleados públicos.
UNDÉCIMA	Estructura organizativa.
DUODÉCIMA	Ejercicio de derechos en materia de Protección de Datos Personales.
DÉCIMOTERCERA	Comunicación de Brechas de Seguridad.
DÉCIMOCUARTA	Medidas de Seguridad.

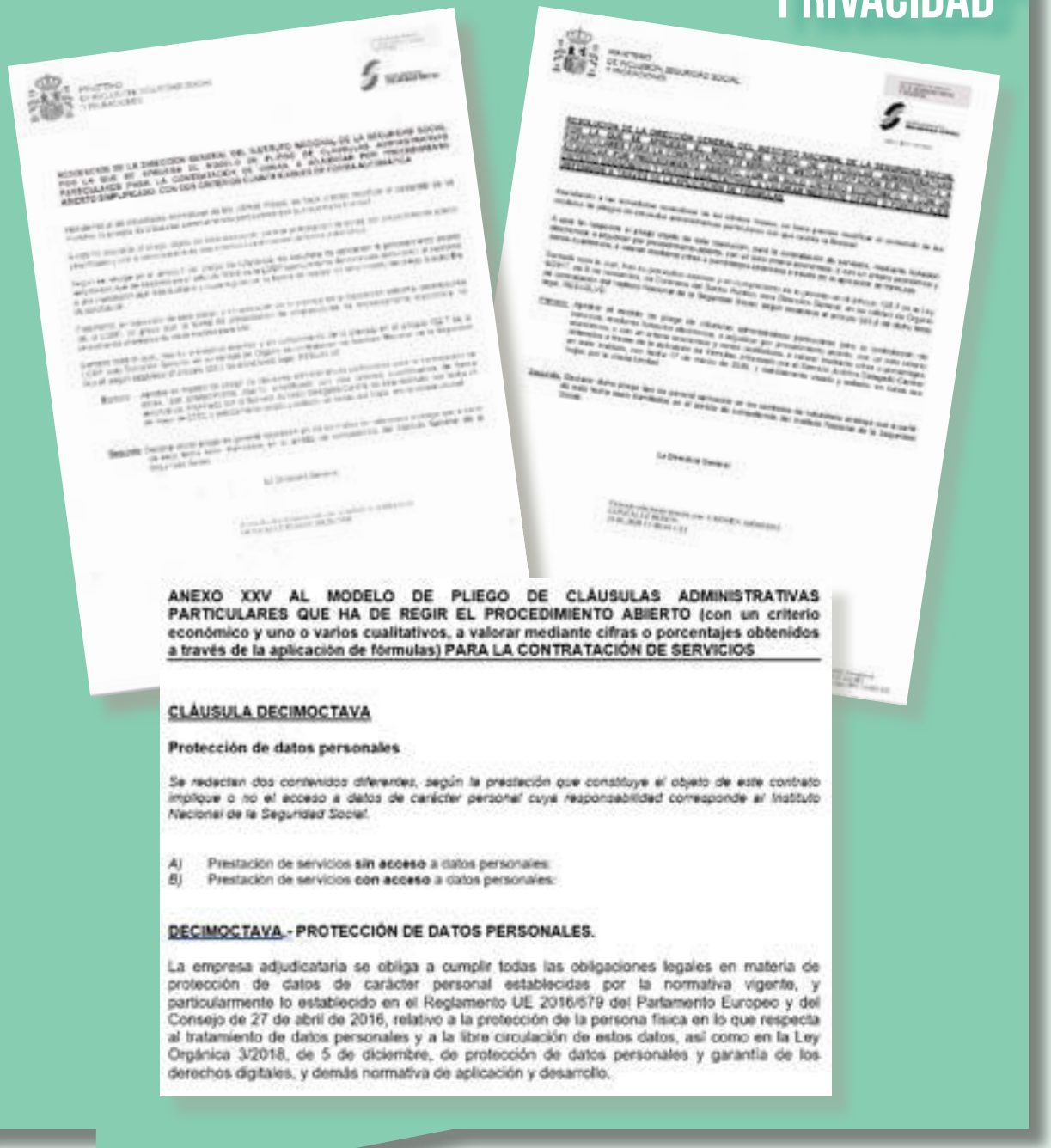
*Para el contenido de todas ver el epígrafe homónimo del apartado de Protección de Datos Personales de la intranet del INSS.

CUADRO 12

(PCAP) la obligación del futuro contratista de respetar la normativa vigente en materia de protección de datos, entre otras medidas.

Para ello se ha procedido a la actualización y aprobación por parte de la Directora General de los diferentes **MODELOS DE PLIEGOS TIPO CONTRACTUALES** elaborados por los servicios centrales de la Entidad, informando de ello a las distintas unidades del Instituto con competencia en materia contractual, debiéndose destacar la cláusula 13.7 referida a las obligaciones genéricas del contratista en materia de protección de datos personales, y sobre todo, el anexo XXV del PCAP referido a la cláusula específica de protección de datos, donde se han establecido dos tipos diferentes de cláusula nº 18 (A y B) en función de que la prestación objeto del contrato implique o no el acceso a datos personales custodiados por la entidad **(VER ANEXO 7 Y CUADRO 13)**

"CONTRATACIÓN PÚBLICA EN EL INSS Y PRIVACIDAD"



ANEXO XXV AL MODELO DE PLIEGO DE CLÁUSULAS ADMINISTRATIVAS PARTICULARES QUE HA DE REGIR EL PROCEDIMIENTO ABIERTO (con un criterio económico y uno o varios cualitativos, a valorar mediante cifras o porcentajes obtenidos a través de la aplicación de fórmulas) PARA LA CONTRATACIÓN DE SERVICIOS

CLÁUSULA DECIMOCTAVA

Protección de datos personales

Se redactan dos contenidos diferentes, según la prestación que constituye el objeto de este contrato implique o no el acceso a datos de carácter personal cuya responsabilidad corresponde al Instituto Nacional de la Seguridad Social.

A) Prestación de servicios **sin acceso** a datos personales.
B) Prestación de servicios **con acceso** a datos personales:

DECIMOCTAVA - PROTECCIÓN DE DATOS PERSONALES.

La empresa adjudicataria se obliga a cumplir todas las obligaciones legales en materia de protección de datos de carácter personal establecidas por la normativa vigente, y particularmente lo establecido en el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de la persona física en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, así como en la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, y demás normativa de aplicación y desarrollo.

CUADRO 13

FASE
PLANIFICACIÓN ESTRATÉGICA Y OPERATIVA

Para llevar a cabo las actuaciones que se habían identificado durante la **FASE DE ÁNALISIS DEL IMPACTO DEL RGPD**, dentro de un enfoque 360º era fundamental que se actuase a todos los niveles organizacionales, de forma que consiguiéramos mayor agilidad en la adaptación y maximizáramos la efectividad de ésta. Por ello el plan de acción se articuló en dos ámbitos que han operado de forma simultánea: el estratégico y el operativo.

>> PLANIFICACIÓN ESTRATÉGICA

La planificación estratégica, la coordinación de actuaciones al máximo nivel entre las Entidades Gestoras y Servicios Comunes que integran la Seguridad Social y el control y revisión de las medidas adoptadas, recae en:

- el Delegado de Protección de Datos de la SESSP
- La Comisión de Protección de Datos de la Administración de la Seguridad Social

todo ello se completa mediante la participación en los grupos de trabajo y las reuniones de alto nivel de diversa índole donde se toman decisiones con impacto en protección de datos y seguridad de los sistemas de información **[VER CUADRO 14].**

>> PLANIFICACIÓN OPERATIVA

Por otra parte, para hacer realidad lo planificado a nivel estratégico e impulsar la ejecución efectiva de las actuaciones identificadas y planificadas a nivel estratégico, se consideró imprescindible reforzar la capacidad de actuación de la figura del SPD del INSS.

Este apoyo se articula, por una parte, de forma permanente a través del asesoramiento especializado y colaboración de la **INSPECCIÓN DE SERVICIOS**, que centraliza todas las actuaciones en la materia a nivel de la Entidad, y por otra, de forma descentralizada, mediante el **GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS (GTPD)** a través del cual, se amplia y ramifica su capacidad de análisis, actuación, control y revisión en todas las áreas de la gestión de la Entidad, con lo que se favorece la eficacia y aplicación homogénea a nivel de todas las subdirecciones.

De esta forma, cada Subdirección General propuso un interlocutor-representante que, además de desempeñar distintas responsabilidades en el concreto ámbito competencial de la Subdirección General de pertenencia, tuvieran conocimiento y experiencia en materia de protección de datos.

La estructura del **GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS (GTPD)** es la que se refleja en el **CUADRO 14**.

CRITERIOS DE SELECCIÓN DE SUS INTEGRANTES

En la **SELECCIÓN DE SUS MIEMBROS** ha primado que aúnen perfiles jurídicos y técnicos, que tengan experiencia en distintos ámbitos, incluido el provincial, y que las responsabilidades que desempeñen respalden la eficacia en la implantación de las medidas adoptadas.

La apuesta y preocupación de la Entidad por la protección de datos también se ve reflejada en el perfil de sus integrantes, con experiencia como Subdirectores Generales, directores provinciales, jefes de área y servicio de un amplio abanico de materias.

GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS

Coordinación Jefa de la Inspección de Servicios

Secretaría Jefe de Área especializado en el programa de protección de datos

Representantes de las áreas

- Secretaría General
- SG de Gestión de Prestaciones
- SG de Gestión de Incapacidad Temporal y Otras Prestaciones a Corto Plazo
- SG de Ordenación y Asistencia Jurídica
- SG de Coordinación de Unidades Médicas
- SG de Gestión Económico-Presupuestaria

CUADRO 14

COMPETENCIAS Y FUNCIONAMIENTO

Este grupo se reúne, como mínimo mensualmente, y tiene como misiones principales:

- Apoyar al SPD en todo lo que les encomiende.
- Elevar propuestas al SPD para su consideración en la Comisión de PD de la SESS.
- Ser interlocutores en sus respectivas subdirecciones generales.
- Impulsar y efectuar el seguimiento de las actuaciones de adaptación al RGPD en cada una de las subdirecciones generales.
- Revisar los procesos de su respectiva subdirección e identificar de áreas de mejora en PD a través de cada uno de sus miembros.
- Aportar la visión práctica y conocimientos desde la perspectiva de su ámbito de competencias.
- Centralizar la recepción y análisis de las consultas e incidencias en materia de PD para dar una respuesta homogénea a éstas en toda la organización.
- Participar en las reuniones de los proyectos de sus respectivos ámbitos de competencia para aportar la visión de la protección de datos desde el diseño.
- Realizar una actividad pedagógica y de concienciación respecto de la PD en sus respectivas unidades.

En las reuniones del GTPD se establecen las actuaciones concretas que cada uno de sus miembros debe realizar para dar cumplimiento a la planificación y cronograma de actuaciones programadas. Estos compromisos y su cumplimiento quedan reflejados en las actas que se confeccionan de cada reunión (véase imagen contigua). En el periodo entre reuniones se mantiene una comunicación fluida entre sus miembros, con la coordinación de la Inspección de Servicios.

ACTA Nº 10 DEL GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL TPD

1. INTRODUCCIÓN

1. ORDEN DEL DIA

2. ASUNTOS GENERALES

3. ACCIONES FUTURAS

4. OTRAS CONSIDERACIONES

En la reunión siguiente, se revisa el grado de ejecución de las tareas encomendadas en las anteriores y se resuelven las cuestiones que se plantean. Se realizan las deliberaciones necesarias sobre los asuntos de la orden del día para adoptar decisiones, establecer criterios o presentar propuestas, y se fijan los objetivos y actuaciones siguientes a realizar por parte de sus miembros y el reparto entre éstos.

El GTPD, además, funciona como un foro de debate y reflexión donde confrontar ideas y puntos de vista en materia de protección de datos y constituye un importante núcleo de detección y análisis de nuevas áreas de mejora y desarrollo de la privacidad en nuestro ámbito competencial de gestión.

>> ACTUACIONES PLANIFICADAS, GRADO DE EJECUCIÓN Y RESULTADOS OBTENIDOS

Las actuaciones planificadas vienen recogidas en el **CRONOGRAMA** resultante tras realizar la fase de **ANÁLISIS DEL IMPACTO DEL RGPD** [ANEXO 4].

En la actualidad prácticamente se han completado en su totalidad de actuaciones previstas en el plazo establecido [TABLA DE RESUMEN DE ACTUACIONES], con buenos resultados desde el punto de vista de la calidad de la protección de la privacidad, y un alto grado de satisfacción por la parte de las unidades de gestión que han acogido de forma muy positiva la reducción de cargas y proceso de racionalización a través del enfoque dual centralización-descentralización.

FASE ACCIÓN

Como ya se explicaba en el apartado dedicado a la **FASE DE ANÁLISIS DEL IMPACTO DEL RGPD** se elaboró un documento que analizaba minuciosamente cada aspecto de la norma y sus implicaciones en nuestra gestión, tomando en consideración todas las actuaciones, sólida infraestructura construida y el vasto conocimiento atesorado, a través de buenas prácticas y la identificación de las áreas de mejora, durante la **FASE EXPERIENCIA**, que representaba un punto de partida ideal en este camino de adaptación y de hacer realidad un enfoque 360º que llegue a todos los puntos y actores de la organización.

A la vista de ello, se recopilaron todas las actuaciones que había que llevar a cabo para completar la adaptación y adoptar plenamente la nueva filosofía en la que se inspira el RGPD.

Esa serie de actividades se priorizaron y programaron dentro de un **CRONOGRAMA** que ha guiado la actuación de los distintos órganos y grupos de trabajo durante la fase de acción. De esos trabajos, la mayor parte se han llevado a término o están próximos a completarse. Es importante subrayar que estas actividades no se consideran como de un sólo acto o ejecución única sino que, como ya se indicaba en el apartado dedicado al valor **AGILIDAD**, son procesos iterativos que buscan una actuación rápida inicial y un perfeccionamiento posterior ciclo a ciclo mediante la revisión y permanente desarrollo, muy en la línea de la filosofía del Reglamento que entiende la labor de velar por la privacidad como un **PROCESO CONTINUO** que implica la permanente evaluación y ponderación de riesgos y la búsqueda incansable de nuevas formas de mejorar la protección y salvaguarda de los datos personales.

En estos momentos, el citado **CRONOGRAMA** muestra el amplio grado de ejecución alcanzado junto con aquellas otras actividades que son de ejecución continuada, como se muestra en la **TABLA RESUMEN DE ACTUACIONES**.

Si bien, son muchas las actuaciones acometidas durante este periodo, se considera que de todo el conjunto de actuaciones, deben destacarse como principales hitos las que se desarrollan a continuación:

1. Impartición de **INSTRUCCIONES A LAS DDPP** sobre diversos aspectos de gran relevancia en materia de protección de datos **[ANEXO 6]**

Para que todo lo analizado y aprendido se lleve a efecto de manera adecuada, la SPD elaboró el documento **"INSTRUCCIONES EN MATERIA DE PROTECCIÓN DE DATOS"** que se encuentra recogido en la INTRANET del INSS.

Este documento, orientado tanto a la actividad prestacional como a las actividades de régimen interno de la Entidad, tiene un contenido eminentemente práctico y establece las directrices en materia de privacidad de los datos a seguir en materias fundamentales como la gestión documental, el bloqueo de acceso a datos de personas especialmente protegidas, el traslado de documentación a otros organismos, los requisitos para la seguridad de las comunicaciones, las cláusulas contractuales de confidencialidad, la identificación de los ciudadanos y de los empleados públicos o la comunicación de brechas de seguridad. Por su importancia se reproduce en **ANEXO 6.**

2. Diseño de **OBJETIVOS INSTITUCIONALES** para reforzar las actuaciones en materia de PD en la red provincial **[ANEXO 7].**

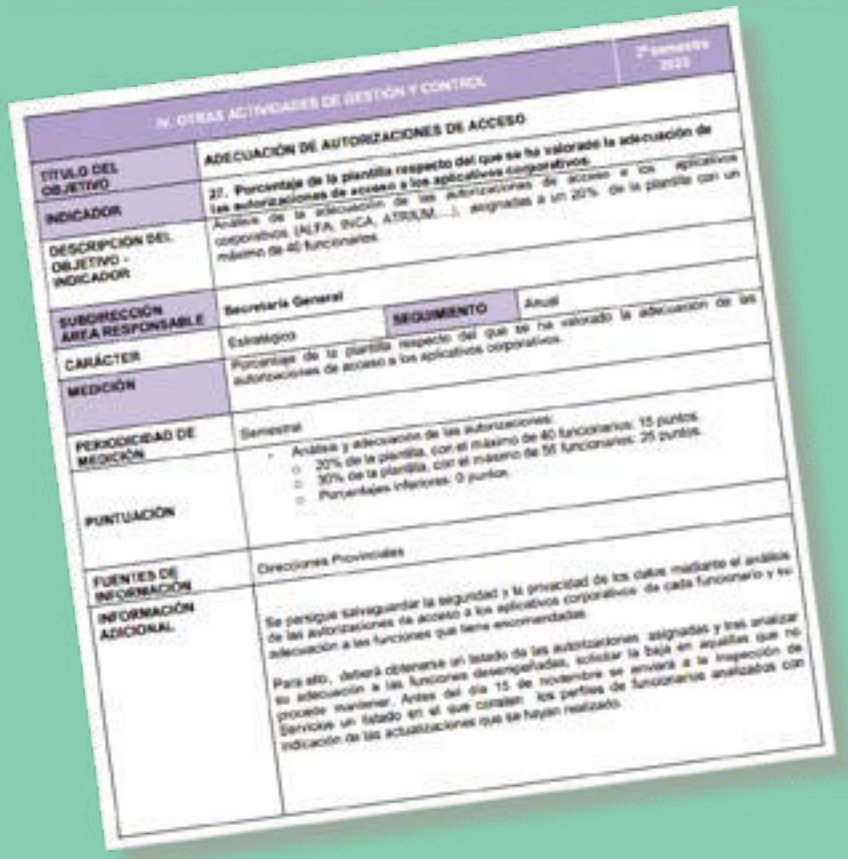
Como ya se indicaba al principio de esta memoria, nuestra Entidad funciona a través de un sistema consolidado y exitoso de **GESTIÓN POR OBJETIVOS** para hacer efectiva la **MISIÓN** de la organización, en plena alineación con la estrategia y que dirige los pasos de la organización hacia el alcance de nuestra **VISIÓN**. Este sistema apuntala otras actuaciones como en el caso de la desarrollada en el punto anterior: la impartición de instrucciones, ya que con la visión y objetivos estratégicos se marca el lugar al que dirigirnos, las instrucciones muestran su concreción más pormenorizada y clarificadora pero la gestión por objetivos pone el acento en la **ACCIÓN**, siendo el motor indispensable para que ese movimiento necesario se produzca en la dirección y con la velocidad adecuadas para hacer realidad todo lo anterior.

Así, con la incorporación de objetivos que respaldan la **POLÍTICA DE PRIVACIDAD** se sitúa a ésta a la misma altura que a aquellas actividades fundamentales para hacer posible y garantizar el cumplimiento de los objetivos estratégicos de la organización, como es el **OBJETIVO DE NO INTERRUPCIÓN DE RENTAS**. Además de situarle en esa posición preminente de máxima relevancia, con ello se refuerza la concienciación a todos los niveles de la organización y se le da visibilidad y se favorece, con todo ello, la interiorización del enfoque 360º.

Tras la entrada en vigor del RGPD se ha continuado con el establecimiento de **OBJETIVOS DIRIGIDOS A GARANTIZAR LA PRIVACIDAD DE LOS DATOS PERSONALES DESDE ESE ENFOQUE 360**, aunando ambición, operatividad y máximo impacto en la mejora de la protección. Para el año 2020 se ha establecido el objetivo: Análisis de la adecuación de las autorizaciones de acceso a los aplicativos y bases de datos corporativas a través de los cuales se accede a los datos personales de los interesados, asignadas a un porcentaje de la plantilla. Con él se persigue **ASEGURAR LA CORRESPONDENCIA Y PERMANENTE ACTUALIZACIÓN DE LAS AUTORIZACIONES DE ACCESO** a los aplicativos que tienen datos personales, con las competencias desempeñadas en cada momento por el autorizado **[CUADRO 15]**.

Todo ello muy ligado con las medidas de seguridad que se explican en la **FASE DE GESTIÓN DE LA PRIVACIDAD Y LA SEGURIDAD** y los ciclos iterativos de **CONTROL Y REVISIÓN**, que también se explican en la respectiva fase.

OBJETIVOS INSTITUCIONALES DEL INSS: EL COMPROMISO ESTRATÉGICO CON LA PRIVACIDAD

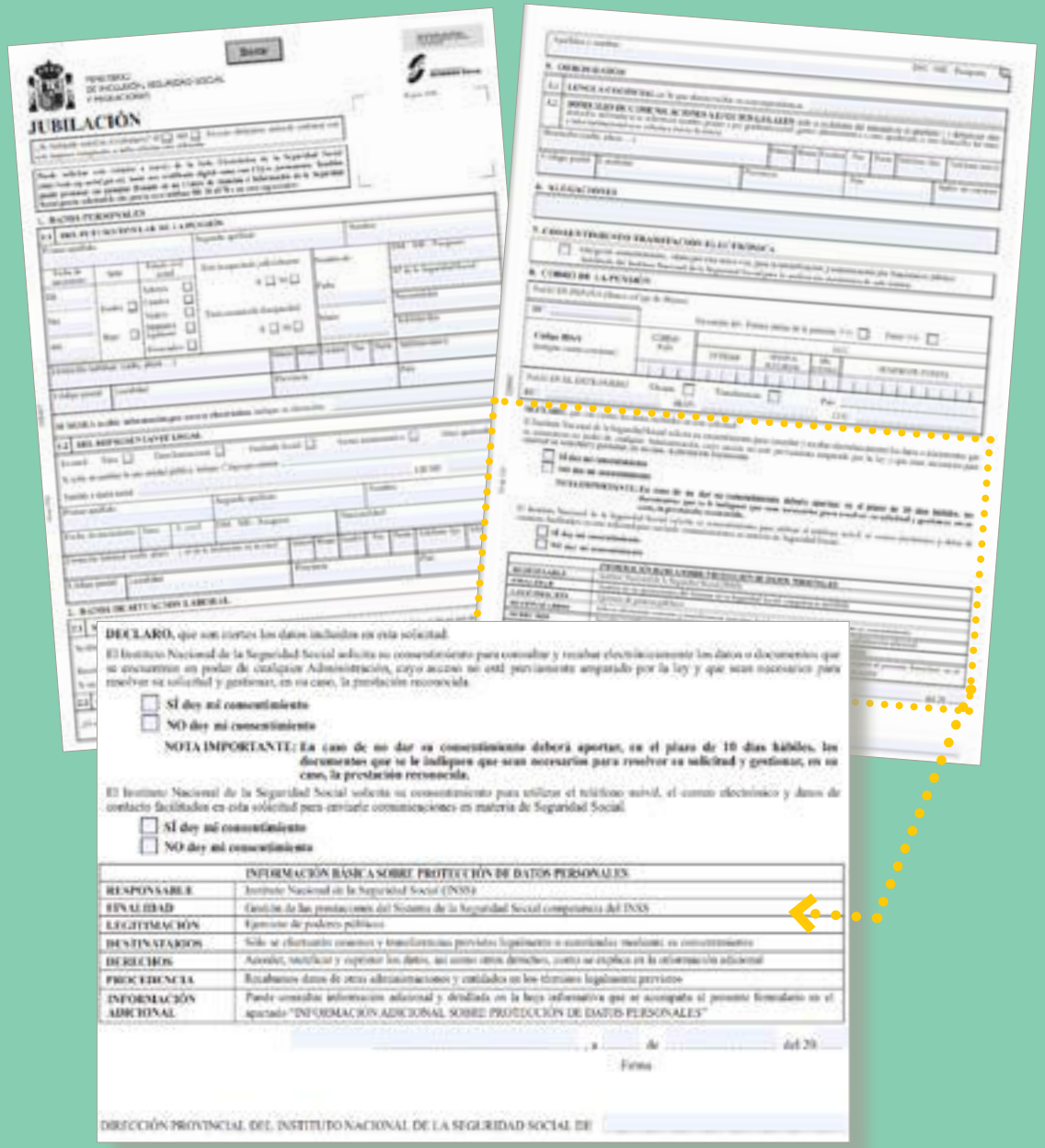


IV. OTRAS ACTIVIDADES DE GESTIÓN Y CONTROL			1º Semestre 2020
TÍTULO DEL OBJETIVO	ADECUACIÓN DE AUTORIZACIONES DE ACCESO		
INDICADOR	27. Porcentaje de la plantilla respecto del que se ha valorado la adecuación de las autorizaciones de acceso a los aplicativos corporativos		
DESCRIPCIÓN DEL OBJETIVO - INDICADOR	Análisis de la adecuación de las autorizaciones de acceso a los aplicativos corporativos (ALFA, INCA, ATRIUM,...), asignadas a un 20% de la plantilla con un máximo de 40 funcionarios.		
SUBDIRECCIÓN ÁREA RESPONSABLE	Secretaría General		
CARÁCTER	Estratégico	SEGUIMIENTO	Anual
MEDICIÓN	Porcentaje de la plantilla respecto del que se ha valorado la adecuación de las autorizaciones de acceso a los aplicativos corporativos.		
PERIODICIDAD DE MEDICIÓN	Semestral		
PUNTUACIÓN	• Análisis y adecuación de las autorizaciones: ○ 20% de la plantilla, con el máximo de 40 funcionarios: 15 puntos. ○ 30% de la plantilla, con el máximo de 56 funcionarios: 25 puntos. ○ Porcentajes inferiores: 0 puntos.		
FUENTES DE INFORMACIÓN	Direcciones Provinciales		
INFORMACIÓN ADICIONAL	Se persigue salvaguardar la seguridad y la privacidad de los datos mediante el análisis de las autorizaciones de acceso a los aplicativos corporativos de cada funcionario y su adecuación a las funciones que tiene encomendadas. Para ello, deberá obtenerse un listado de las autorizaciones asignadas y tras analizar su adecuación a las funciones desempeñadas, solicitar la baja en aquellas que no procede mantener. Antes del día 15 de noviembre se enviará a la Inspección de Servicios un listado en el que consten los perfiles de funcionarios analizados con indicación de las actualizaciones que se hayan realizado.		

OBJETIVO: ADECUACIÓN DE AUTORIZACIONES DE ACCESO				
Indicadores de medición	**Descripción**	**Fuente de datos**	**Carácter/Puntuación**	**Área responsable**
27. Porcentaje de la plantilla respecto del que se ha valorado la adecuación de las autorizaciones de acceso a los aplicativos corporativos.	Análisis de la adecuación de las autorizaciones de acceso a los aplicativos corporativos (ALFA, INCA, ATRIUM,...), asignadas a un 20% de la plantilla con un máximo de 40 funcionarios.	Direcciones Provinciales	ESTRATÉGICO Puntos: 15-25	SECRETARÍA GENERAL

CUADRO 15

DEBER DE INFORMACIÓN: EJEMPLO DE INFORMACIÓN EN DOBLE CAPA


JUBILACIÓN

DECLARO, que son ciertos los datos incluidos en esta solicitud.

El Instituto Nacional de la Seguridad Social solicita su consentimiento para consultar y recabar electrónicamente los datos o documentos que se encuentren en poder de cualquier Administración, cuyo acceso no esté previamente amparado por la ley y que sean necesarios para resolver su solicitud y gestionar, en su caso, la prestación reconocida.

☐ **SÍ doy mi consentimiento**

☐ **NO doy mi consentimiento**

NOTA IMPORTANTE: En caso de no dar su consentimiento deberá aportar, en el plazo de 10 días hábiles, los documentos que se le indiquen que sean necesarios para resolver su solicitud y gestionar, en su caso, la prestación reconocida.

El Instituto Nacional de la Seguridad Social solicita su consentimiento para utilizar el teléfono móvil, el correo electrónico y datos de contacto facilitados en esta solicitud para enviarle comunicaciones en materia de Seguridad Social.

☐ **SÍ doy mi consentimiento**

☐ **NO doy mi consentimiento**

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS PERSONALES	
RESPONSABLE	Instituto Nacional de la Seguridad Social (INSS)
FINALIDAD	Gestión de las prestaciones del Sistema de la Seguridad Social competencia del INSS
LEGITIMACIÓN	Ejercicio de poderes públicos
DESTINATARIOS	Sólo se efectuarán cesiones y transferencias previstas legalmente o autorizadas mediante su consentimiento
DERECHOS	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional
PROCEDENCIA	Recabamos datos de otras administraciones y entidades en los términos legalmente previstos
INFORMACIÓN ADICIONAL	Puede consultar información adicional y detallada en la hoja informativa que se acompaña al presente formulario en el apartado "INFORMACIÓN ADICIONAL SOBRE PROTECCIÓN DE DATOS PERSONALES"

, a de del 20

Firma

DIRECCIÓN PROVINCIAL DEL INSTITUTO NACIONAL DE LA SEGURIDAD SOCIAL DE

INFORMACIÓN ADICIONAL SOBRE PROTECCIÓN DE DATOS PERSONALES

RESPONSABLE DEL TRATAMIENTO	***¿Quién es el responsable del tratamiento de sus datos personales?*** Instituto Nacional de la Seguridad Social C/ Padre Damián, 4 CP 28036 Madrid, ESPAÑA https://sede.segsocial.gob.es
DELEGADO DE PROTECCIÓN DE DATOS	***¿Cómo puede contactar con el Delegado de Protección de Datos?*** Dirección del Servicio Jurídico de la Seguridad Social C/ Segunda, 13 - 4ª Planta CP 28004 Madrid, ESPAÑA https://sede.segsocial.gob.es
FINALIDAD DEL TRATAMIENTO	***¿Para qué utilizaremos sus datos?*** Sus datos serán tratados con la finalidad principal de resolver esta solicitud y de gestionar, en su caso, la prestación reconocida. El tratamiento de sus datos de contacto tendrá como finalidad la realización de comunicaciones y remisión de información en materia de Seguridad Social. Los datos personales proporcionados se conservarán mientras sean necesarios para gestionar su prestación y las de sus posibles beneficiarios así como para otros fines de archivo y estadística pública.
LEGITIMACIÓN DEL TRATAMIENTO	***¿Cuál es la legitimación para el tratamiento de sus datos?*** El tratamiento de los datos se realizará sobre la base del ejercicio de poderes públicos autorizado por una norma legal (Arts. 66, 71, 72, 77 y concordantes Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social, en adelante, TRLGSS). Por lo que respecta a las comunicaciones y envío de informaciones en materia de Seguridad Social, el tratamiento tendrá legitimado por su consentimiento. La negativa a otorgarlo supondrá que no podrá recibir este tipo de envíos, si bien, no impedirá que le podamos informar por dichos canales del estado de sus solicitudes. También le informamos de que no está obligado a facilitar su *dirección de correo electrónico y número de teléfono móvil y que, en caso de no facilitarlos,* no impedirá el trámite de su solicitud.
DESTINATARIOS DE CESIONES O TRANSFERENCIAS	***¿A quién comunicaremos sus datos?*** Los datos personales obtenidos por el Instituto Nacional de la Seguridad Social en el ejercicio de sus funciones tienen carácter reservado y sólo se utilizarán para los fines encomendados legalmente, sin que puedan ser cedidos o comunicados a terceros, salvo que la cesión o comunicación tenga por objeto alguno de los supuestos previstos expresamente en el artículo 77 del TRLGSS así como en los supuestos indicados en cualquier otra norma de rango legal. Si se trata de una solicitud basada en normativa internacional, sus datos podrán ser cedidos a los organismos extranjeros competentes para el trámite de su solicitud.
DERECHOS DE LAS PERSONAS INTERESADAS	***¿Cuáles son sus derechos cuando nos facilita sus datos personales?*** Respecto de los datos personales proporcionados, puede ejercitar en cualquier momento y en los términos establecidos por la normativa de protección de datos los derechos de acceso, rectificación, supresión, limitación y oposición, o bien retirar el consentimiento prestado a su tratamiento en los casos que hubiese sido requerido, todo ello mediante escrito presentado en un Centro de Atención e Información de la Seguridad Social (CAISS) o, por correo postal o a través de la sede electrónica de la Seguridad Social, ante el Delegado de Protección de Datos cuyos datos se encuentran en el segundo apartado de esta tabla. Le informamos de que en caso de considerar que su requerimiento no ha sido atendido apropiadamente, tiene la posibilidad de presentar una reclamación ante la Agencia Española de Protección de Datos.
PROCEDENCIA	***¿Cómo obtenemos sus datos personales?*** Además de los datos facilitados por usted en su solicitud recabamos otros datos personales de otras administraciones y entidades en cumplimiento de la normativa y con el fin de agilizar y facilitar la actuación administrativa. Estos accesos a datos están amparados en normas con rango de ley.

www.seg-social.es https://sede.seg-social.gob.es

3. **PROMOCIÓN DE LA FORMACIÓN, INFORMACIÓN Y LA DIVULGACIÓN DE LA MATERIA DE PROTECCIÓN DE DATOS.**

Dentro del enfoque 360º que orienta nuestra actuación, es fundamental realizar una ambiciosa planificación de la **PROGRAMACIÓN DE LOS CURSOS FORMATIVOS** de protección de datos para asegurar la progresiva formación de todo el personal en esta materia, y apoyar ese esfuerzo formativo con otro divulgativo a través de la edición de materiales didácticos.

Desde mayo de 2018, fecha de entrada en vigor del RGPD hasta la actualidad, se han desarrollado **52 EDICIONES** del Curso Protección de datos de carácter personal, con un total de **863 ASISTENTES**. La ambiciosa programación que se está realizando persigue culminar en **2022** la formación de la **TOTALIDAD DE LA PLANTILLA**. Para asegurar el cumplimiento de este objetivo se promoverá el establecimiento de nuevos objetivos institucionales en esta línea de actuación.

4. Implementación de la **PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO** en los proyectos de desarrollo de aplicaciones corporativas del INSS (base de datos de gestión documental -SARTIDO-, Registro electrónico centralizado, Tarjeta Social Digital e IMV).

5. **MEJORA DE LA PRIVACIDAD EN EL ACCESO A LOS SERVICIOS DE ATENCIÓN NO PRESENCIALES** mediante la revisión y refuerzo de los protocolos de identificación para la atención telefónica y telemática. Para ello se está desarrollando un proyecto que, una vez culminado, permitirá relacionarnos con los ciudadanos en idénticas condiciones y con las mismas garantías que por la vía presencial a través del resto de canales de atención.

Para ello se está trabajando sobre todos los niveles de acceso a la información actuales y se están sentando las bases para poder ampliarlos en el futuro de forma paralela al refuerzo de los sistemas de identificación fehaciente

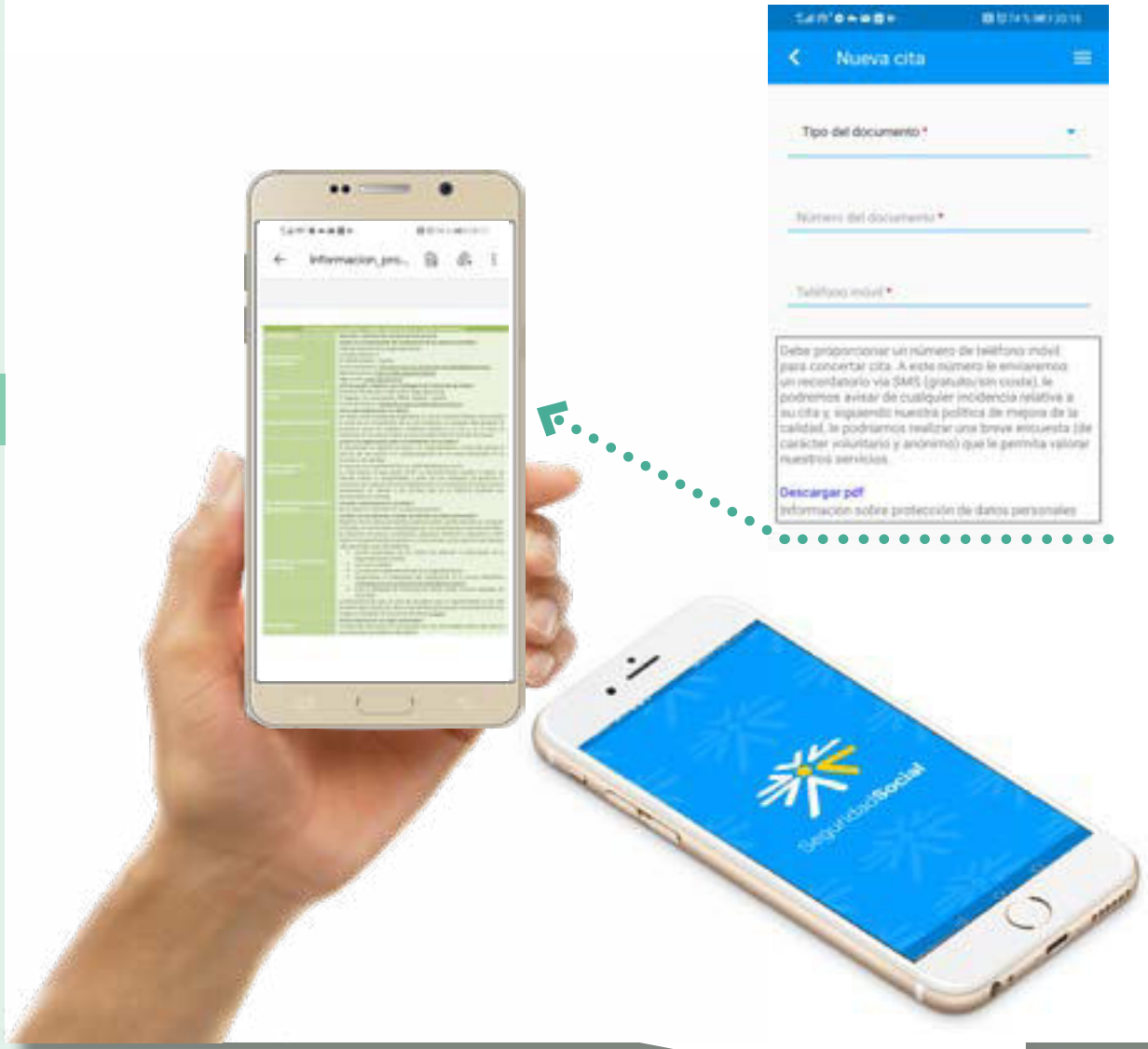
Dentro de todos los mecanismos de identificación que incluye ese proyecto, destacan por el grado de avance de su desarrollo, la integración de los sistemas OTP (one time password o contraseña de un sólo uso mediante mensaje SMS) en las herramientas de gestión de apoyo a la atención telefónica (CRM) o el uso de medios de videollamada.

Además, el protocolo e instrucciones de identificación para la información personalizada de nivel básico está en permanente revisión y adecuación. Un ejemplo de ello ha sido la puesta en marcha y aplicación de lo anterior a la **NUEVA LÍNEA DE ATENCIÓN E INFORMACIÓN ESPECÍFICA (L900) PARA LA NUEVA PRESTACIÓN DEL INGRESO MÍNIMO VITAL (IMV).**

En este sentido debe destacarse la complejidad que conllevaba la asunción de este proyecto en el marco y plazos que debió acometerse (mayo 2020). Durante ese breve espacio de tiempo se trabajó a contrareloj para hacer posible la atención de una previsible demanda desbordante, por ello debió recurrirse a un encargo a medios propios. Para articular ese servicio, además de otras actividades necesarias, se prestó especial atención a la relativa a la **GARANTÍA DE LA PRIVACIDAD EN TÉRMINOS IDÉNTICOS** a los que aplicamos para la labor informativa cotidiana prestada por personal funcionario. El resultado de esa labor de análisis y diseño del servicio se plasmó en el **CLAUSULADO DEL ENCARGO** y en una serie de actuaciones adicionales (instrucciones y pautas) para reforzar y garantizar la protección de la privacidad en el caso de una prestación que tiene en cuenta situaciones personales que requieren de la máxima protección (tales como la condición de ser víctima de violencia de género o de trata de seres humanos o encontrarse en una situación de exclusión social) **ANEXO 8.**

Por ello, se reforzó el **PROTOCOLO DE IDENTIFICACIÓN** y se dedicó una parte importante de la **FORMACIÓN** al personal informador sobre la materia, además de facilitar distintos materiales de apoyo y soporte. También merecen especial atención las **INSTRUCCIONES** impartidas por la SPD concretando y especificando de forma pormenorizada los aspectos incluidos de forma sucinta en la redacción del Encargo y su clausulado de protección de datos **[ANEXO 6]**.

DEBER DE INFORMACIÓN:
EJEMPLO EN LA APP DE SEGURIDAD SOCIAL



CUADRO 17

Con motivo de la **PRÓRROGA** del servicio, se decidió reorientarlo para ampliar la tipología de atenciones e informaciones que se podían prestar, incluyendo las de carácter personalizado.

La puesta en marcha de ese servicio supuso revisar nuevamente el protocolo, actualizarlo, establecer un perfilado muy riguroso basado en el **PRINCIPIO DE MINIMIZACIÓN DE DATOS** y adaptar el clausulado para incorporar garantías adicionales.

Por último, también se estableció un **PROCEDIMIENTO REFORZADO DE ATENCIÓN A PERSONAS CON DATOS PROTEGIDOS**, llevado a cabo exclusivamente por funcionarios autorizados (que ejercen cargos de responsabilidad en el centro de trabajo donde se prestan estos servicios). Con ello se consigue que estos interesados puedan acceder al servicio sin reducir la especial protección que éstos, por sus especiales circunstancias, requieren en un contexto en el que el acceso a los servicios presenciales es más limitado debido a las medidas de contención de la pandemia.

6. Elaboración de un **MAPA DE LA PROTECCIÓN DE DATOS DE LA ENTIDAD** identificando todas las tareas y puntos a revisar en caso de ulteriores modificaciones de la normativa de protección de datos.

Toda la revisión que se ha realizado con motivo de la adaptación al RGPD y la adopción del enfoque 360º ha servido para detectar todos los ámbitos en los que un cambio normativo de calado como este puede afectar. De esta forma se ha adoptado una medida proactiva para recopialr y "cartografiar" todos esos puntos para crear un mapa de la protección de datos de la Entidad que facilite

cualquier actualización o revisión posterior y que pueda apoyar cualquier toma de decisiones o planificación, facilitando con agilidad una información precisa, completa y actualizada sobre la materia.

7. DEBER DE INFORMACIÓN Y FORMATO DE DOBLE CAPA:

Durante la fase de acción se procedió, en primer lugar, a adaptar el **MODELO DE DOBLE CAPA** propuesto desde la AEPD a las especialidades de nuestro ámbito y, posteriormente, a aplicar este formato de doble capa a todos los formularios y modelos en los que era aplicable, empezando por los que se utilizan por parte de los ciudadanos, concretamente **101 FORMULARIOS EN FORMATO DIGITAL Y PAPEL,** para añadir después los de consumo interno en materia de RRHH fundamentalmente.

8. Deber de informar y videoconferencias.

Debido a la actual situación de crisis sanitaria se ha adaptado la función inspectora mediante el uso de medios telemáticos (videoconferencia). Por este motivo entre la información que se envía a las DDPP que van a ser objeto de inspección se incluye la cláusula informativa en materia de protección de datos **(ANEXO 10)**.

Además, también se han adaptado las **VERSIONES ELECTRÓNICAS** de los formularios y las aplicaciones que registran datos personales (plataforma Tu Seguridad Social y aplicación móvil, **[CUADROS 17 Y 18]** para que se adecúen a las exigencias actuales. Del mismo modo se ha procedido con la adecuación de las locuciones automatizadas de nuestros servicios de atención telefónica.

Por último, también se ha participado en la revisión y actualización del apartado de información de protección de datos en la **WEB** con motivo de la adaptación al RGPD y revisado y ampliado el contenido relativo a la privacidad en nuestra **INTRANET** corporativa.

DEBER DE INFORMACIÓN: EJEMPLO EN EL ESPACIO DE AUTOGESTIÓN "TU SEGURIDAD SOCIAL"

CUADRO 18

TABLA RESUMEN DE LAS PRINCIPALES ACTUACIONES DE ADAPTACIÓN REALIZADAS

ACTUACIONES PLANIFICADAS Y GRADO DE EJECUCIÓN ALCANZADO	PORCENTAJE 25 · 50 · 75 · 100
Designación del DPD	
Acuerdo del perfil más apropiado para dar apoyo al DPD o y constitución de la unidad de apoyo	
Regulación de su funcionamiento	
Fórmulas de colaboración y comunicación entre unidades	
Creación del Grupo de Trabajo de PD. Regulación de su composición y funcionamiento	
Delimitación del concepto «tratamiento»	
Establecimiento de criterios homogéneos para la identificación de las bases legales para el tratamiento	
Análisis del alcance jurídico del Considerando 43	
Estudio especial de los casos basados en el consentimiento	
Estudio de aquellos consentimientos que no cumplan con la nueva norma, su posible sustitución por otra base jurídica u obtención de los nuevos consentimientos. Determinar y desarrollar los mecanismos para acreditar que se ha otorgado el consentimiento	
Estudio especial de los casos en los que los datos no se obtienen directamente de los interesados (cesión legítima de datos)	
Estudio de los tratamientos relativos a la gestión de los recursos humanos, con especial atención a las infracciones y sanciones administrativas y si se cumplen las condiciones para dicho tratamiento	
Análisis del alcance jurídico del régimen de protección de datos en caso de tratamientos de datos de menores y el posible impacto de éste en nuestra gestión	
Verificación y, en su caso, adaptación –técnica, instrucciones, modificaciones en los procesos que sea necesario- a lo establecido en la LO respecto de la identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos	
Realizar los análisis de riesgos de los tratamientos existentes y que puedan realizarse en el futuro	
Determinación de las medidas de seguridad a aplicar previa valoración de las medidas aplicadas hasta la fecha, desde el nuevo enfoque del riesgo para los derechos y libertades de los interesados (diligencia, autolimitación, valoración del mantenimiento o supresión de los documentos de seguridad, auditorías bienales, objetivos institucionales, aplicabilidad de la medida de seguridad de seudonimización en nuestro ámbito	
Articulación del sistema para demostrar la eficacia de las medidas implantadas y determinar la forma en que se garantizará que quienes acceden a los datos sólo pueden hacerlo conforme a las instrucciones impartidas por el responsable.	
Llevar a cabo las EIPD (agrupándose, en su caso) cuando el análisis de riesgos sobre el tratamiento determine la existencia de un alto riesgo desde la perspectiva de los derechos y libertades de los interesados.	
Determinación de medidas de seguridad aplicables o elevación de consulta, en su caso.	
Seguimiento de las decisiones institucionales relativas a la consideración como tratamientos de alto riesgo a efectos de EIPD	
Implantación de las medidas que se hayan determinado según el resultado del análisis de riesgo y, en su caso, de la EIPD	
Definición de qué constituye una violación o quiebra de seguridad.	
Protocolos de actuación (posible edición de instrucciones o guías para la casuística más frecuente) y, en su caso, notificación.	
Establecer la forma de documentación y registro de las violaciones o quiebras de seguridad detectada	

ACTUACIONES PLANIFICADAS Y GRADO DE EJECUCIÓN ALCANZADO	PORCENTAJE 25 · 50 · 75 · 100
Análisis de la situación previa existente: ficheros declarados ante la AEPD a nivel centralizado y descentralizado, a los efectos de la regularización y depuración de los ficheros declarados y, en su caso, en proceso de inscripción	
Determinación del nivel de agregación/desagregación (funcional y geográfica) que va a aplicarse.	
Aplicación de este criterio y obtención de un listado de tratamientos: Registro de actividades de tratamientos	
Elaboración y publicación por medios electrónicos del Inventario de actividades de tratamiento	
Comunicar las modificaciones que se produzcan en el registro de actividades de tratamiento al DPD.	
Establecimiento correspondencias entre ficheros SIGLA-tratamientos RGPD.	
Adaptación (principio de transparencia e información) y rediseño (a efectos de ubicación y visibilidad de la información), en su caso, de todos los formularios de captación de datos en sus múltiples y diversos formatos: papel, electrónicos, telefónicos, aplicaciones y entorno web. A efectos tanto de cláusulas informativas (doble capa) como de obtención de consentimiento	
Aplicación, en su caso, a los tratamientos de datos internos respecto de nuestro personal	
Articular los mecanismos para acreditar que se ha cumplido con el deber de informar	
Comprobación de que se cumple con el deber de informar en el caso de videovigilancia	
Estudio de los nuevos derechos ARCO+ y su régimen de ejercicio	
Desarrollo de mecanismos para su ejercicio, en caso de ser de aplicación	
Elaboración de un Protocolo de derechos ARCO+	
Edición de formularios para el ejercicio de derechos ARCO+	
Publicación en la Intranet corporativa y en el aplicativo CAISSGestiona de los formularios de ejercicio de derechos ARCO+	
Difusión del Protocolo de derechos ARCO+ entre el personal de la Entidad	
Información y formularios del Protocolo de derechos ARCO+ por medios electrónicos	
Edición de un díptico informativo sobre el ejercicio de derechos ARCO+ para los interesados	
Contratación administrativa. Adaptación de las cláusulas de confidencialidad	
Detección de la existencia de encargos de tratamiento no regularizados	
Revisión o elaboración, en su caso, de los contratos de encargo de tratamiento (o acto administrativo, cuando proceda) en función de la aplicabilidad de la nueva LOPD	
Adaptación a las premisas del contenido y regulación del encargo de tratamiento de la norma reguladora de las competencias de la GISS	
Dictado de instrucciones para la selección de encargados de tratamiento que ofrezcan las garantías establecidas en la norma	
Revisión del clausulado y pliegos tipo especifícos para los contratos en los que haya encargos de tratamiento	
Implementación de la Protección de Datos desde el Diseño y por Defecto en los proyectos de la entidad	ACTUACIONES DE EJECUCIÓN PERMANENTE
Emisión de instrucciones generales (ámbito centralizado y descentralizado)	
Acciones de comunicación interna	
Impartición de formación	
Impartición de instrucciones y habilitación de los procesos necesarios, en su caso, para la verificación de datos personales que obren en poder de las AAPP declarados en por los interesados	
Creación de un buzón corporativo único (interno y externo) para los asuntos y consultas relacionadas con la PD a nivel de toda la organización	
Difusión e instrucciones del nuevo procedimiento centralizado de PD	
Elaboración y mantenimiento de un repositorio de consultas de PD	
Publicación en la intranet corporativa del repositorio de consultas y difusión de la medida entre el personal	

FASE

EVOLUCIÓN DEL UNIVERSO DE LA PROTECCIÓN DE ATLAS DE LOS TRATAMIENTOS DE DATOS PERSONALES

Como ya se mencionó brevemente para ilustrar el valor **EFICIENCIA**, una de las primeras y más importantes actuaciones dentro de la adaptación a la nueva norma de nuestro Instituto fue la transformación del antiguo esquema de 1450 ficheros registrados ante la Agencia Española de Protección de Datos (AEPD) al actual Registro de Actividades de Tratamiento [RAT] (e IAT publicado en la página web de la Seguridad Social).

Para asegurar el éxito del proceso de transformación fue clave:

- por una parte, un análisis pormenorizado, respaldado con la experiencia inspectora acumulada a través del programa de inspección de protección de datos, de todos y cada uno de los 1450 ficheros provinciales y centralizados registrados hasta el cierre del Registro de la Agencia, así como,
- por otra, un estudio de todos los procesos relacionados con datos personales efectuados por la Entidad tanto a nivel central como periférico, tomando como base el mapa de procesos del INSS **[CUADRO 20]**, y
- la definición y delimitación del contenido de los conceptos afines a "tratamiento de datos personales" que íbamos a aplicar en la transformación en aras de la racionalización de su contenido y estructura, considerando pros y contras de ese enfoque y las consecuencias de su adopción en su posterior gestión y actualización permanentes.

En la primera fase de análisis, procedimos a cuestionarnos si la estructura actual basada en un esquema de ficheros vinculados principalmente a aplicaciones informáticas y bases de datos que daban apoyo auxiliar a algunos de los tratamientos principales que se realizan en la organización respondía a las siguientes cuestiones:

- si existía una correspondencia entre los antiguos ficheros y el concepto vigente de tratamiento
- si daba cobertura a todos los tratamientos que se derivan de los procesos que dan soporte a la actividad gestora competencia del INSS y si esta cobertura era plena
- si la atomización de ficheros incidía en una mejor protección de los datos personales que se tratan, en mayores garantías de los derechos y libertades de los ciudadanos en esta materia y en el cumplimiento de las obligaciones que se derivan del Reglamento
- si esa organización incidía positiva o negativamente en los posteriores flujos de control, revisión y actualización

De ese análisis se concluyó que la estructura anterior no respondía a las nuevas necesidades ni a los principios rectores de este proceso de transformación, por lo que se desechó y se construyó un nuevo esquema.

Para ello se ha aplicado la **FILOSOFÍA DE LA REINGENIERÍA RADICAL DE PROCESOS**. De tal forma que el registro:

- se ha construido desde cero para prescindir de conceptos desactualizados y otros lastres conceptuales
- se ha organizado de forma centralizada

DATOS DEL INSS:

para asegurar la **HOMOGENEIDAD** y **EFICIENCIA** en este proceso

- se ha basado en la aplicación de un concepto de tratamiento transversal e integrador orientado por la filosofía de la gestión por procesos.

Así, se tomó como punto de partida el **MAPA DE PROCESOS** de la Entidad, y se procedió a analizar y estudiar pormenorizadamente :

- cada uno de los macrotratamientos que se realizan en la organización,
- los microtratamientos que incluían,
- la forma en que se organiza la gestión de unos y otros y,
- su distribución y organización geográfica y funcional.
- El esquema de responsabilidades de cada tratamiento en los dos circuitos, el centralizado y el periférico, así como su posible solapamiento y supuestos de corresponsabilidad.

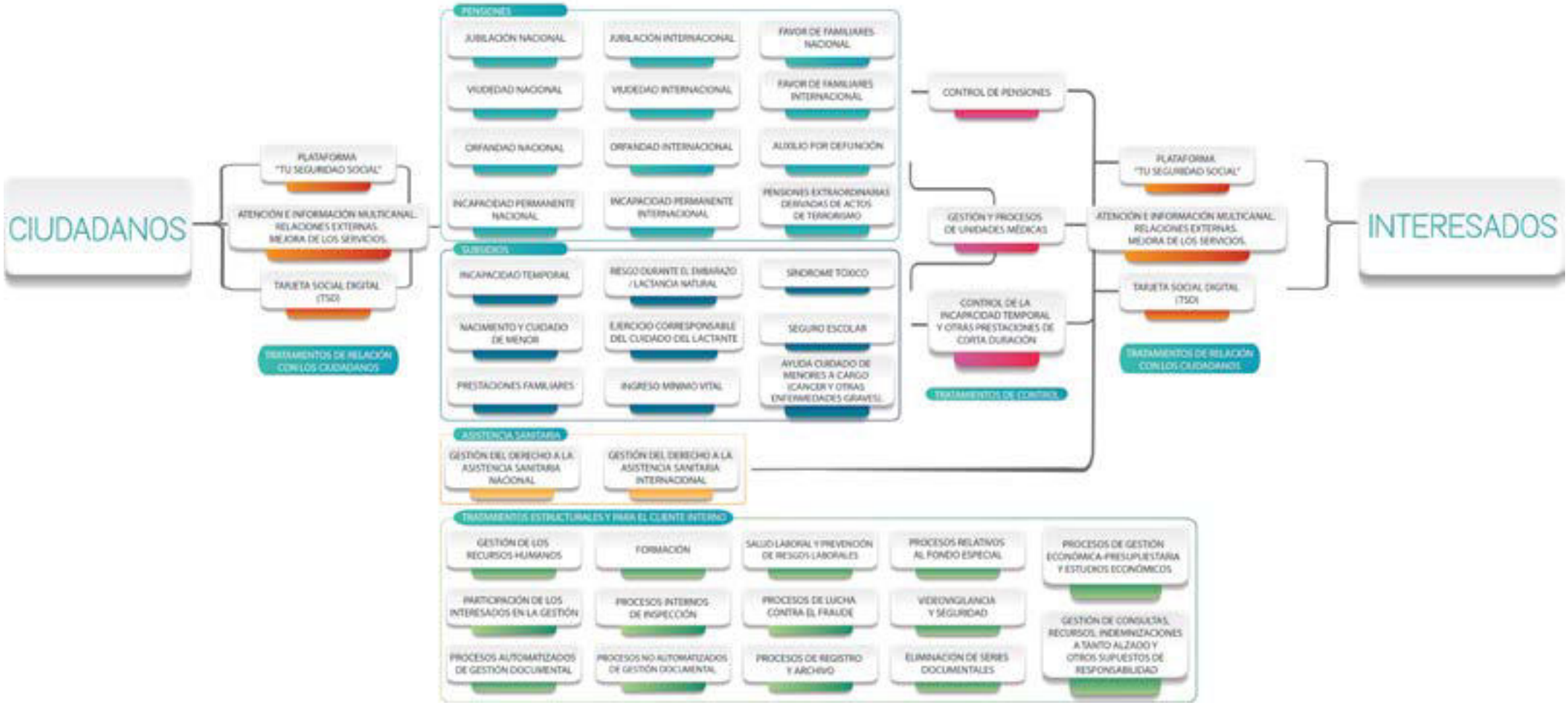
Una vez finalizado ese proceso, se ha revisado el acomodo de cada uno de los ficheros y microtratamientos, previamente registrados ante la Agencia, en su macrotratamiento correspondiente

REGISTRO DE ACTIVIDADES DE TRATAMIENTO E INVENTARIO PUBLICADO EN LA WEB DE LA SEGURIDAD SOCIAL

CUADRO 19

MAPA DE PROCESOS

DEL INSTITUTO NACIONAL DE LA SEGURIDAD SOCIAL



CUADRO 20

y, posteriormente, se ha trasladado esta información, en formato de **TABLA DE CORRESPONDENCIAS**, a cada una de las unidades responsables de dichos ficheros, para su seguimiento y control **[CUADRO 21]**.

Este costoso proceso de racionalización tiene numerosas **VENTAJAS** a efectos de:

- Facilitar su gestión y actualización posterior, estableciendo un **CRITERIO SISTEMATIZADO** para incorporar posibles nuevos tratamientos futuros (como ha ocurrido en 2020 con la aprobación del IMV)
- Hacer más **COMPRENSIBLE**, tanto a nivel interno como externo, su estructura, al alinearse los tratamientos con los procesos fundamentales de nuestra gestion, tanto prestacionales como de caracter interno de la organización incluyendo los orientados al personal de la Entidad.
- Asegurar que el modelo construido abarca la **TOTALIDAD** de los tratamientos realizados por nuestro Instituto en todos sus ámbitos de gestión y distribución geográfica, pues a través de este enfoque no queda ningún tratamiento, por pequeño o poco frecuente que sea y con independencia del ámbito geográfico y funcional en el que se realice dentro de la organización, que no esté identificado y respaldado por su correspondiente registro.
- Todo ello de forma **EFICIENTE** pues sustituye los costosos procesos iterativos y exhaustivos de detección, análisis, mantenimiento, control y auditoría enfocados a cada microproceso (ficheros) considerado de forma aislada y descontextualizada, por la identificación de macroprocesos suficientemente amplios para dar cabida a todos los posibles microprocesos que se efectúan pero a la vez lo suficientemente acotado como para hacer de cada uno un conjunto manejable, comprensible, sistemático, lógico y de fácil estructura e identificación de responsabilidades.

Como resultado de ello se diseñó un esquema de **43 MACROTRATAMIENTOS** que aglutina todas y cada una de las operaciones de tratamiento y subtratamientos (antiguos ficheros declarados) que se llevan a cabo en este Instituto **[CUADRO 6]**.

Gracias a ello, se ha pasado de gestionar y actualizar un conjunto registrado en SIGLA de más de 1450 ficheros radicados a nivel provincial y, por tanto, distribuidos por todo el territorio nacional, que se caracterizaban por:

- haber sido creados según un criterio algo dispar y heterogéneo y
- encontrarse lastrado por la consideración limitada y restrictiva del concepto de fichero más propia de normativas anteriores

a un Registro de Actividades de Tratamiento lógico y sistemático, con 43 tratamientos (o macrotratamientos coincidentes con los procesos fundamentales y fácilmente identificables de la gestión del INSS). **(CUADRO 20)**

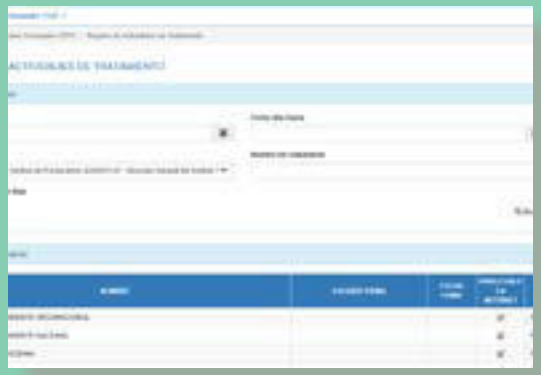
El **SISTEMA DE REPARTO DE RESPONSABILIDADES** también aplica una lógica fácil y clara que permite identificar el responsable de cada operación de tratamiento en función del ámbito funcional y geográfico en que se haya realizado. Por una parte, en función de la materia que corresponde según el reparto competencial que rige nuestra actividad y, por otra, en función de si esa operación ha sido llevada a cabo por personal destacado en los servicios centrales o en los periféricos. De tal forma que si la operación de tratamiento que deba analizarse ha sido realizada como parte de una actuación centralizada, la responsabilidad de ésta recaerá en el responsable de la unidad que haya realizado ese tratameinto centralizado o de áquel del que dependa el funcionario que lo haya llevado a cabo. Por su parte, si la operación en cuestión ha sido llevada a cabo por parte del personal de la red periférica, será responsable el que ostenta ese cargo en el ámbito provincial.

Para poder comprender la **APARENTE SIMPLICIDAD DE LA ESTRUCTURA DE MACROTRATAMIENTOS** es preciso ahondar en su complejidad intrínseca que parte de un conocimiento profundo y preciso de los procesos y las operaciones y tareas que las componen.

El esquema que se ha diseñado parte de una disección de cada proceso en cada una de las suboperaciones y subtareas que implica para determinar cuáles estarán englobadas dentro de un tratamiento y cuáles dentro de otro. Así, por ejemplo, si utilizamos el **PROCESO DE JUBILACIÓN** (prestación clave de nuestro sistema) debemos entender que el inicio del proceso de jubilación se produce:

- en el momento de la primera información al ciudadano y que luego va acumulando todas las operaciones de:
- captura de la solicitud,
- escaneado de documentación,
- recopilación de los datos de bases de

LA TRANSFORMACIÓN HACIA EL NUEVO RAT DEL INSS
EQUIVALENCIAS Y REGISTRO EN ASSI



CUADRO 21

datos corporativas propias y ajenas (p.ej. del Servicio Público Estatal de Empleo),

- trámitación,
- notificación,
- reclamación administrativa y/o judicial,
- pago,
- control y mantenimiento de la prestación
- así como todos los contactos informativos que se produzcan durante su amplio ciclo de vida, incluso una vez se ha tramitado la pensión.

Todas esas operaciones van a corresponder al tratamiento jubilación que estemos analizando. Cuando, en cambio, analicemos los procesos de, por ejemplo, **ATENCIÓN E INFORMACIÓN EN SU CONJUNTO,** entonces hablaremos del tratamiento de atención multicanal. De ta forma que el esquema funciona como una **TABLA DE DOBLE ENTRADA**, en función del enfoque y perspectiva del análisis que le necesitemos dar, cubriendo tanto los **PROCESOS CENTRALIZADOS COMO LOS PERIFÉRICOS.**

En algunos casos, se decidió **DESDOBLAR** algunos procesos por dar mayor relevancia a algún aspecto diferenciador, como es el de las prestaciones internaconales.

Por último, agunos tratamiento, por su especificidad se decidió establecer como un tratamiento independiente por su singularidad y relevancia como es el caso de la plataforma **TU SEGURIDAD SOCIAL** o la **TARJETA SOCIAL DIGITAL**.

FASE

GESTIÓN DEL CONOCIMIENTO, FORMACIÓN Y CONCIENCIACIÓN

LA PROTECCIÓN DE DATOS PERSONALES: UN ESPACIO DESTACADO EN LA INTRANET DEL INSS

La INTRANET institucional cuenta con un espacio específico que pretende ser un punto de información de fácil acceso, en el que poder encontrar respuesta y ayuda ante las diversas dudas o inquietudes que puedan surgir al personal de la entidad, en materia de protección de datos personales.

Este apartado se estructura en los siguientes epígrafes:

PRESENTACIÓN

En ella se vincula la protección de los datos personales con los artículos 18.4 de la Constitución Española, 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea y 16.1 del Tratado de Funcionamiento de la Unión Europea, y se cita el RRGPD, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y la LOPDGDD, como disposiciones reguladoras de este materia.

Se incluye en este apartado un tríptico **[CUADRO 22]** sobre protección de datos que se entrega junto con el resto de documentación bienvenida al personal de nuevo ingreso en el INSS, como medida de concienciación e información del nivel de responsabilidad que supone para los nuevos usuarios que van a acceder de forma intensiva a una ingente cantidad de datos personales entre los que se incluyen datos especialmente sensibles.

NORMATIVA

Donde se establecen enlaces a los diarios oficiales y boletines en los que se publican las principales disposiciones reguladoras de esta materia.

PROTECCIÓN DE DATOS EN EL INSS

Este epígrafe incluye:

- La Guía de protección de datos del INSS
- Las instrucciones impartidas por la SPD.
- Un repositorio de las consultas efectuadas y de las respuestas adoptadas en esta materia.
- La documentación relacionada con las auditorías.
- Un enlace al procedimiento e instrucciones comunes para toda la Seguridad Social.
- El procedimiento de confidencialidad (bloqueo/marcaje de datos).

BRECHAS DE SEGURIDAD

Se incluyen instrucciones específicas para la gestión de las brechas de seguridad en el INSS, así como un enlace al documento **"DETECCIÓN Y COMUNICACIÓN DE BRECHAS DE SEGURIDAD EN LA SEGURIDAD SOCIAL".**

ATENCIÓN AL EJERCICIO DE DERECHOS RGPD

Está integrado por:

- Instrucciones para la tramitación de los derechos de protección de datos en el INSS.
- Instrucciones de tramitación en el ámbito de la Seguridad Social.
- Formularios para el ejercicio de los derechos.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

En él se explica la normativa que sustenta la obligación de llevar a cabo el Registro y se incluyen los siguientes enlaces:

INFORMACIÓN Y CONCIENCIACIÓN: TRÍPTICO INFORMATIVO

DEFINICIONES DE TÉRMINOS BÁSICOS Y FUNDAMENTALES EN MATERIA DE PROTECCIÓN DE DATOS

NORMATIVA BÁSICA DE REFERENCIA

DECÁLOGO DE BUENAS PRÁCTICAS

INFORMACIÓN SOBRE LA ESTRUCTURA DE TRATAMIENTOS DE LA ORGANIZACIÓN

OBLIGACIONES DE LA ENTIDAD

RECORDATORIOS Y CONSIGNAS PARA LA CONCIENCIACIÓN

DERECHOS DE LOS EMPLEADOS

RESPONSABILIDADES

INFORMACIÓN ADICIONAL SOBRE PROTECCIÓN DE DATOS

Al inventario de actividades de tratamiento del INSS publicado en la web de la Seguridad Social **[ANEXO 1]**

A la tabla de equivalencias entre los ficheros SIGLA del INSS y los nuevos tratamientos **[CUADRO 21]**.

DELEGADA Y SUBDELEGADA DE PROTECCIÓN DE DATOS

Se explican las, funciones y competencias de ambas figuras, así como las estructuras articuladas para darles soporte, y se incluye un índice de las consultas formuladas a la DPD y de las respuestas adoptadas por la misma.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Se indica cuáles son las funciones de la AEPD, y se incluye:

- Una relación de las **RESOLUCIONES DE INTERÉS DE LA AEPD** sobre Protección de Datos Personales relacionados con las AAPP
- Una relación de **INFORMES DE LA AEPD** relacionados con los tratamientos de datos de las AA.PP.

FORMACIÓN

Este apartado contiene:

- El material didáctico del **"CURSO DE PROTECCIÓN DE DATOS"** impartido por el INSS.
- El apartado **"RECURSOS PEDAGÓGICOS"**, donde se incluye una tabla informativa en la que se diferencian los distintos tipos de solicitudes de datos que puede recibir el INSS, y una serie de recomendaciones aplicables al teletrabajo, a las actividades desarrolladas en las Unidades Médicas y para la prevención de delitos en materia de PD.

VIOLENCIA DE GÉNERO

Por el carácter especialmente sensible de los datos personales de las personas afectadas por violencia de género y la importancia de informar y concienciar de las especiales medidas de seguridad que deben aplicarse para garantizar los derechos de estas víctimas, se decidió incluir un apartado específico sobre este tema en la Intranet. En él se contienen los siguientes **DOCUMENTOS**:

- La Guía de Protección de Datos y Prevención de Delitos (AEPD)
- La Guía de derechos de las mujeres víctimas de violencia de género, de la Delegación del Gobierno para la violencia de Género.
- Responsabilidad Administrativa, Disciplinaria, Civil y Penal por la difusión/revelación de contenidos-datos sensibles (AEPD)
- La protección de datos como garantía en las políticas de prevención del acoso (AEPD).

Y **ENLACES** a los siguientes contenidos:

- Solicitud de retirada de contenidos distribuidos en la red.
- Delegación del Gobierno para la violencia de género.
- Policía Nacional.
- Guardia Civil.
- Web de recursos de apoyo y prevención ante casos de violencia de género (WRAP).
- Servicio telefónico de atención y prevención a las víctimas de violencia de género.
- Instituto de la Mujer y para la igualdad de oportunidades.
- Línea de ayuda en ciberseguridad.

BUZÓN DE CONSULTAS

En pleno siglo XXI y ante una sociedad altamente digitalizada e interconectada, el uso de las tecnologías de información y comunicación deviene en una obligación para el conjunto de las administraciones públicas.

Precisamente en base a ello, y con el fin de lograr una mayor eficiencia y eficacia en la gestión de los tiempos de respuesta y las soluciones dadas a las dudas, consultas o problemas surgidos

NÚMERO DE CONSULTA:	17

Nº de Registro de Inspección: BLV-10.03.20-OUR

PALABRAS CLAVE

Certificado de pensionista, solicitud por autorizado, domicilio de envío

CONSULTA

Recibida una solicitud de certificado de pensionista, presentada por una empresa financiera crediticia en calidad de autorizada, existiendo dudas sobre la firma manuscrita del pensionista, ¿a qué domicilio ha de enviarse el certificado?

RESPUESTA

En relación con la presente consulta, analizada la misma y teniendo en cuenta que nos demandabais: "indicaciones de cómo proceder al tratarse de solicitudes que, aunque a simple vista reúnen los requisitos exigidos, se han realizado presumiblemente con un *"consentimiento aparentemente viciado" del representado y sin su verdadera firma"*, se **expone**:

UNO. Los funcionarios de este Instituto no pueden dedicarse a realizar actuaciones de peritaje caligráfico para asegurar la autenticidad de las firmas manuscritas aportadas en las solicitudes y autorizaciones presentadas en nuestros registros (cosa distinta es que se detecte una evidente discordancia entre la firma manuscrita del interesado y la de su DNI).

DOS. Desde el punto de vista de la protección de datos personales, debemos adoptar una actitud proactiva, buscando siempre garantizar la integridad, confidencialidad y disponibilidad de los datos personales que este Instituto utiliza y custodia.

TRES. Así pues, como medida de seguridad oportuna para garantizar la confidencialidad de los datos personales, está el enviar los certificados, informes, resoluciones y demás comunicaciones que se mantengan con los beneficiarios de las prestaciones competencia del INSS, al domicilio de dichos interesados y que nos conste en nuestros sistemas de información, a efectos de notificaciones.

CUATRO. Así mismo, se recuerda que en la información suministrada en la propia sede electrónica en el servicio electrónico *"Solicitud de certificado de prestaciones (como representante)"* se puntualiza que *"Por parte del Instituto Nacional de la Seguridad Social se enviará al domicilio del interesado el certificado solicitado"*. Debiéndose entender por tal domicilio, tal como habitualmente venís haciendo (salvo el caso concreto del cual nos habéis informado), el que nos conste en nuestros sistemas de información, a efectos de notificaciones.

Por todo ello, cabe **CONCLUIR**:

PRIMERO. Salvo que se observe la falta de algún requisito, o la firma manuscrita del pensionista sea manifiestamente incompatible con la de su DNI, se deberán seguir tramitando dichas solicitudes y expidiendo sus correspondientes certificados.

SEGUNDO. En todo caso, los certificados deberán remitirse al domicilio del pensionista, y NUNCA al de la empresa financiera. De esta forma aseguramos la confidencialidad de los datos personales contenidos en dichos certificados, en el hipotético caso de que se hubieran falsificado las firmas y/o solicitudes del pensionista.

NORMATIVA CLAVE

- Reglamento (UE) 2016/679, General de Protección de Datos;
- LO 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales.
- RDL 8/2015, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social;
- Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas.

CUADRO 23

en la gestión ordinaria del INSS, se acordó crear un buzón centralizado destinado en exclusiva a la resolución de las consultas planteadas por el conjunto de las 52 direcciones provinciales y las distintas subdirecciones generales que integran esta entidad.

BUZÓN DE CONSULTAS EN MATERIA DE PROTECCIÓN DE DATOS EN EL INSTITUTO NACIONAL DE LA SEGURIDAD SOCIAL

consultas.inss-sscc.proteccion-de-datos@seg-social.es

Con ello se ha logrado establecer un mecanismo ágil y eficaz a través del cual dar una respuesta rápida y común a las dudas surgidas en la interpretación y aplicación de la normativa de protección de datos, dotando de uniformidad a la implementación práctica de la misma en los distintos procedimientos de gestión administrativa competencia de la entidad, y muy especialmente, en aquellos relacionados con los datos personales y los derechos de los ciudadanos que mantienen algún tipo de relación con el INSS.

Este buzón está asignado en cuanto a su llevanza y supervisión a la Inspección de servicios de la entidad, encargándose del mismo de forma directa un jefe de área y una inspectora de servicios, siempre bajo la supervisión directa de la Jefa de la inspección de servicios, y contando con el apoyo del GTPD del INSS, foro ante el cual se plantean las consultas de mayor complejidad, acordando por el conjunto de sus integrantes las respuestas o soluciones a implementar.

Como referencia hay que mencionar que a lo largo del 2019 se han atendido **52 CONSULTAS** formuladas por las Direcciones Provinciales, en relación con la aplicación de la normativa de protección de datos. Asimismo se han atendido **4 REQUERIMIENTOS POR DENUNCIAS CIUDADANAS** ante la Agencia Española de Protección de Datos.

GUÍA DE PROTECCIÓN DE DATOS

Entre la información que se incluye en el apartado "Protección de datos en el INSS" **(ANEXO 11),** en la INTRANET institucional, la **GUÍA DE PROTECCIÓN DE DATOS** compendia las directrices y orientaciones fundamentales sobre la materia:

Se trata de un documento de 66 páginas a través del que se trata de ofrecer a todos los trabajadores de la entidad la información más relevante y con un enfoque práctico para facilitar la aplicación real y comprensión de esta materia.

A continuación se reproduce el **ÍNDICE DE CONTENIDOS** en el que se listan las cuestiones que se abordan en el cuerpo del documento:

- **PRESENTACIÓN**
- **CONCEPTOS Y DEFINICIONES**
  - ¿QUÉ ES UN TRATAMIENTO DE DATOS PERSONALES?
  - ¿QUIÉN ES EL RESPONSABLE DEL TRATAMIENTO DE DATOS
  - ¿QUIÉN ES EL ENCARGADO DEL TRATATAMIENTO DE DATOS
  - ¿CUÁLES SON LOS PRINCIPIOS APLICABLES AL TRATAMIENTO DE DATOS
- **ADECUACIÓN AL RGPD DE LOS TRATAMIENTOS DEL INSS**
  - IDENTIFICACIÓN DE LA LEGITIMACIÓN EN EL TRATAMIENTO DE DATOS PERSONALES
  - CUMPLIMIENTO DEL PRINCIPIO DE TRANSPARENCIA: EL DERECHO DE INFORMACIÓN EN LA RECOGIDA DE DATOS PERSONALES
  - LA TRANSICIÓN DEL REGISTRO DE FICHEROS AL REGISTRO DE TRATAMIENTOS
  - SEGURIDAD EN EL TRATAMIENTO DE LOS DATOS PERSONALES
  - PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

NÚMERO DE CONSULTA	RESUMEN DE LA CONSULTA
CONSULTA 1	Sobre la articulación del derecho de acceso a la información pública con el derecho a la privacidad de las retribuciones del personal, así como la posibilidad de cesión de dichos datos a los representantes sindicales.
CONSULTA 2	Sobre la cesión al autorizado RED de datos personales relativos a deudas por descuentos indebidos practicados a un trabajador en situación de IT en modalidad de pago delegado.
CONSULTA 3	Sobre la necesidad de solicitar autorización del empleado para el tratamiento de sus datos personales en la tramitación de una comisión de servicios.
CONSULTA 4	Sobre la cesión de información sanitaria de un trabajador por parte del INSS, actuando como su empleador, a otra administración pública.
CONSULTA 5	Sobre el ejercicio del derecho de supresión de los datos de contacto, a solicitud del interesado.
CONSULTA 6	Sobre la cesión de datos de formación de los empleados al Servicio de prevención de riesgos laborales.
CONSULTA 7	Sobre la cesión de datos a un Consulado con el fin de comprobar si se ha iniciado el trámite de los expedientes en dicho país.
CONSULTA 8	Sobre la cesión de datos de salud a las CC.AA. para la realización de actuaciones conjuntas en el seguimiento de enfermedad profesional y en la Prevención de Riesgos Laborales.
CONSULTA 9	Sobre la cesión de datos del Registro de Prestaciones Sociales Públicas a la administración local para el trámite de ayudas sociales de su competencia.
CONSULTA 10	Sobre la cesión de datos personales a ISFAS ante una posible incompatibilidad de prestaciones de diferentes regímenes.
CONSULTA 11	Sobre la falta de consentimiento del interesado en los formularios de solicitud de prestaciones respecto a la consulta de información y al envío de comunicaciones.
CONSULTA 12	Sobre la cesión de datos personales ante peticiones de información por las Fuerzas y Cuerpos de Seguridad del Estado, sin mandamiento judicial.

CUADRO 24

- EL DELEGADO DE PROTECCIÓN DE DATOS (DPD) DE LA SEGURIDAD SOCIAL
- TRANSFERENCIAS INTERNACIONALES DE DATOS
- CONFIDENCIALIDAD Y SECRETO PROFESIONAL. RESPONSABILIDADES DE USUARIOS

DERECHOS DE LOS AFECTADOS

- CARACTERÍSTICAS GENERALES
- DERECHOS DE ACCESO
- DERECHO DE RECTIFICACIÓN
- DERECHO DE SUPRESIÓN
- DERECHO DE OPOSICIÓN
- DERECHO A LA LIMITACIÓN DEL TRATAMIENTO
- DERECHO A LA PORTABILIDAD DE LOS DATOS
- DERECHO A NO SER OBJETO DE DECISIONES INDIVIDUALES AUTOMATIZADAS
- PROCEDIMIENTO DE ACTUACIÓN ANTE SOLICITUDES DE EJERCICIO DE DERECHOS
- TUTELA DE DERECHOS ANTE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

PREGUNTAS FRECUENTES

- TRATAMIENTO DE DATOS EN EL MARCO FUNCIONARIAL Y LABORAL
- VIDEOVIGILANCIA
- ACCESO A EXPEDIENTES ADMINISTRATIVOS Y LEY DE TRANSPARENCIA

REPOSITORIO

Con el fin de facilitar la aplicación práctica y homogénea (otro de los valores que ha regido este proceso de adaptación) de la vigente normativa de protección de datos personales en el ámbito concreto de la gestión del INSS, se decidió la creación y configuración de un **REPOSITORIO DE CONSULTAS REALES** planteadas por distintos centros y funcionarios que integran la Entidad.

En este espacio centralizado común para toda la organización, se ha procedido a almacenar, organizar, actualizar y difundir aquellas cuestiones de carácter más significativo, estructurando las mismas en un **FORMATO DIDÁCTICO** para facilitar con ello su comprensión y aplicación práctica ante situaciones iguales o semejantes, difundiendo con ello la importancia de la protección de datos personales en el ámbito de la Seguridad Social y los trámites de gestión asociados a nuestra administración.

Para ello se ha diseñado y adoptado un formato de **FICHAS INFORMATIVAS** en las que de forma breve se pueda difundir la cuestión práctica planteada, la respuesta acordada y el fundamento jurídico de la misma, destacando las palabras clave sobre las que versa la cuestión **[CUADRO 23]**.

Así pues, este repositorio de carácter **DINÁMICO** se va incrementando periódicamente con la incorporación de nuevas fichas informativas y la revisión de las ya publicitadas con el fin de mantener actualizados los conocimientos de los empleados de la Entidad, y orientar a los mismos ante las diversas situaciones reales que se pueden encontrar en sus unidades de gestión a la hora de compaginar las funciones propias de su actividad de administrativa y la implementación de las normas y políticas de protección de datos vigentes y establecidas por el INSS.

Como **EJEMPLOS** más significativos de las fichas informativas que en la actualidad integran el repositorio destacan las que se incluyen en el **CUADRO 24** como resumen de consultas en materia de protección de datos planteadas por las DDPP.

CURSOS DE PROTECCIÓN DE DATOS Y PONENCIAS CURSO SELECTIVO

Como se ha indicado, el INSS incluye en sus **PLANES DE FORMACIÓN** cursos de protección de datos dirigidos a todo el personal de la Entidad. A través de esta oferta se pretende concienciar a los empleados acerca de la importancia del conocimiento y cumplimiento de la normativa reguladora de esta materia y dotarles de los recursos necesarios para desarrollar sus competencias dentro de este marco normativo.

OFERTA FORMATIVA:

CURSOS PRESENCIALES

Estos cursos, de 15 horas de duración, están configurados de una manera eminentemente práctica. Estos cursos están orientados a la aplicación de los conocimientos impartidos en el entorno del INSS, y se desarrollan por expertos en la materia. En ellos se abordan las siguientes cuestiones:

- Normativa reguladora de la protección de datos personales
- Ámbitos subjetivo y objetivo de aplicación
- Conceptos más importantes
- Principios establecidos en el RGPD
- Derechos de las personas y su ejercicio
- Obligaciones de los responsables y encargados del tratamiento
- Funciones y competencias del Delegado de Protección de Datos

CURSOS EN LA INTRANET

Además, en la INTRANET común a toda la Seguridad Social, se incluye de manera permanente el curso: **"CONCIENCIACIÓN. POLÍTICA DE USO SEGURO DE LOS SISTEMAS DE INFORMACIÓN"**, cuyo objetivo es concienciar a los usuarios de una forma práctica y amena, con un enfoque cercano y un toque desenfadado, para acercar una materia tracidionalmente considerada compleja y poco amable [ejemplo de contenidos de uno de estos cursos en el **CUADRO 25**], de la necesidad de utilizar de modo seguro los sistemas de información, conforme se indica en la **POLÍTICA DE USO SEGURO** aprobada de acuerdo a lo especificado por el **ESQUEMA NACIONAL DE SEGURIDAD**.

Está dirigido al personal funcionario y laboral perteneciente a la Secretaria de Estado de la Seguridad Social, y a él se puede acceder, sin necesidad de requisitos previos, por todo el personal, a través de un enlace habilitado de forma permanente.

PONENCIAS DE LOS CURSOS SELECTIVOS

En los cursos selectivos de ingreso a los cuerpos de Gestión y Superior de Técnicos de la Administración de la Seguridad Social, se imparten ponencias sobre protección de datos personales, que se complementan con ejercicios prácticos sobre la materia. Una vez concluido el curso, se efectúa una evaluación dirigida a comprobar que se acredita el nivel de conocimiento exigido.

A través de estos recursos formativos se persigue que todos los funcionarios que ingresan en entidades dependientes de la SESSP dispongan del conocimiento y concienciación necesarios para garantizar la protección de los datos personales que maneja la Seguridad Social.

PILDORAS INFORMATIVAS

Atendiendo a la proactividad que propugna el RGPD y a aprovechando la cultura formativa que el INSS tiene establecida respecto sus empleados, se ha decidido potenciar la difusión de contenidos educativos/formativos en el ámbito de la protección de datos personales.

Así pues, además de los cursos de formación continua en protección de datos planificados tanto por las direcciones provinciales como por la Subdirección General de Recursos Humanos y Materiales, tal como se ha expuesto en el punto anterior, se ha considerado acertado elaborar fichas educativas denominadas “Píldoras Informativas” que de forma breve y esquemática vienen a informar de aspectos concretos en materia de protección de datos.

Como ejemplos pueden citarse las siguientes píldoras informativas **(CUADRO 26)**:

- Decálogo de recomendaciones para el Teletrabajo y la Protección de Datos Personales.
- Comunicación de Brechas de Seguridad de Protección de Datos Personales.
- Decálogo de Protección de Datos para el personal sanitario y administrativo de las Unidades Médicas del INSS.
- Tipos de Derecho de Acceso – Solicitudes de Datos en el INSS.

CUADRO 26

FASE
GESTIÓN DE LA SEGURIDAD Y PRIVACIDAD

1. PARTICIPACIÓN DEL INSS EN EL COMITÉ DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN:

La gestión de la privacidad y de la seguridad son entidades distintas con objetivos comunes: salvaguardar los derechos y libertades de las personas y garantizar la seguridad de la información.

La disposición adicional primera de la LOPDGDD establece que los responsables enumerados en el artículo 77.1 de la ley (entre los que se encuentran las entidades gestoras de la Seguridad Social y el resto de organismos adscritos a la Secretaría de Estado de la Seguridad Social y pensiones) deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el **ESQUEMA NACIONAL DE SEGURIDAD,** así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado. Y que en los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

Con anterioridad a la publicación de esta disposición, varios **HITOS** han marcado el desarrollo del proceso de seguridad en el ámbito de la Seguridad Social:

>> La Orden de 28 de octubre de 2011 creó el **COMITÉ DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (CUADRO 28)** del Ministerio de Trabajo e Inmigración, como órgano colegiado de carácter transversal, adscrito a la Subsecretaría de Trabajo e Inmigración, al que le corresponde determinar y coordinar el mandato contenido en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) y, por tanto, la política de seguridad que se ha de implementar en el Departamento para la utilización de los medios electrónicos de forma que se garantice una adecuada protección de la información.

>> Posteriormente, la Orden de 30 de julio de 2012, del Ministerio de Empleo y Seguridad Social aprobó la **POLÍTICA DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN** del citado Departamento, con la finalidad de proteger adecuadamente todos los sistemas, y garantizar que prestarán sus servicios y custodiarán la información, de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas.

>> Finalmente, la Orden de 7 de mayo de 2014, del Ministerio de Empleo y Seguridad Social creó el **COMITÉ DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA SEGURIDAD SOCIAL (CSISS),** con la función de coordinar todas las actividades relacionadas con la seguridad de los sistemas de información en el ámbito de la Secretaría de Estado y de comunicarse con el **COMITÉ DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DEL MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL (CSTIC)**.

Específicamente se le atribuyeron las siguientes **FUNCIONES**:

1. Definir y elevar para su aprobación al CSTIC los planes estratégicos, líneas de actuación y objetivos en materia de seguridad en la Secretaría de Estado de la Seguridad Social, siempre alineados con la misión y objetivos de la organización.
2. Garantizar la divulgación de la política de seguridad en el ámbito de la Secretaría de Estado de la Seguridad Social.

COMITÉ DE SEGURIDAD Y SISTEMAS DE INFORMACIÓN DE LA SEGURIDAD SOCIAL

PRESIDENTE SECRETARIO DE ESTADO DE LA SEGURIDAD SOCIAL Y PENSIONES *O EL GERENTE DE GISS*

VOCALES UN REPRESENTANTE DESIGNADO POR LOS TITULARES DE CADA UNO DE LOS SIGUIENTES ÓRGANOS:

- GABINETE DE LA SECRETARÍA DE ESTADO DE LA SEGURIDAD SOCIAL Y PENSIONES.
- DIRECCIÓN GENERAL DE ORDENACIÓN DE LA SEGURIDAD SOCIAL.
- INTERVENCIÓN GENERAL DE LA SEGURIDAD SOCIAL.
- INSTITUTO NACIONAL DE LA SEGURIDAD SOCIAL.
- TESORERÍA GENERAL DE LA SEGURIDAD SOCIAL.
- INSTITUTO SOCIAL DE LA MARINA.
- SERVICIO JURÍDICO DE LA ADMINISTRACIÓN DE LA SEGURIDAD SOCIAL.
- GERENCIA DE INFORMÁTICA DE LA SEGURIDAD SOCIAL.

CUADRO 27

3. La aprobación y seguimiento de las normas y procedimientos en materia de seguridad que afecten transversalmente a la Administración de la Seguridad Social.
4. Establecer, cuando sea posible, criterios comunes de actuación en todos los órganos directivos de la organización para el cumplimiento de las normas o procedimientos en materia de seguridad de la información que sean de aplicación.
5. Revisar el estado global de la seguridad en cada uno de los organismos adscritos y órganos y unidades dependientes orgánicamente de la Secretaría de Estado, y elevar los informes pertinentes al CSTIC cuando sea necesario.
6. Trasladar las directrices que sean establecidas desde el CSTIC a cada uno de los órganos directivos y garantizar su cumplimiento.
7. Actualizar y asignar las funciones y obligaciones de cada uno de los responsables definidos en la política de seguridad en la utilización de medios electrónicos en la Administración de la Seguridad Social.
8. Promover las líneas de trabajo para una adecuada concienciación y formación en materia de seguridad para el personal de la Secretaría de Estado de la Seguridad Social.
9. Ser informado, deliberar e intercambiar información con los organismos adscritos y órganos y unidades dependientes orgánicamente de la Secretaría de Estado y que sean responsables de ficheros con datos personales para tratar y asesorar sobre las medidas de seguridad técnica aplicables en los sistemas y servicios que les afecten y que utilicen tecnologías de la información y comunicaciones.

COMPOSICIÓN

El CSSISS se compone de los miembros que se señalan en el **CUADRO 27.**

A través de la integración en este órgano colegiado, el INSS ha **PARTICIPADO** en la adopción de diversas normas, guías y procedimientos, entre los que destacan:

- "Política de uso seguro de los sistemas de información de la Seguridad Social" (por su especificidad se desarrolla en el apartado siguiente).
- "Revisión del uso de los sistemas de información de la Seguridad Social y tratamiento de evidencias electrónicas"
- "Gestión de la Seguridad"
- "Gestión de incidentes de seguridad"
- "Comunicación de incidentes de seguridad"
- "Brechas en tratamientos con datos personales"
- "Apertura de interfaces de datos en ordenadores.
- "Normas, procedimientos y guías de gestión de usuarios".
- "Asignación de perfil especial de Internet"
- "Control de acceso a servicios electrónicos"
- "Seguridad física en oficinas"

Estas normas y procedimientos se encuentran alojados en el apartado **"PROTECCIÓN DE SISTEMAS DE INFORMACIÓN"** de la INTRANET común a todas las entidades, y se accede a ellos desde el apartado **"PROTECCIÓN DE DATOS PERSONALES"** de la INTRANET del INSS, a través de enlaces establecidos al efecto.

[NO PUEDE EXISTIR PRIVACIDAD DE LOS DATOS PERSONALES SIN UNA CORRECTA POLÍTICA Y ESTRUCTURA DE SEGURIDAD DE LA INFORMACIÓN QUE LA HAGA POSIBLE Y VELE DE FORMA DECIDIDA Y CONSTANTE POR ELLA]

COMITÉ DE SEGURIDAD DE LAS TIC
DE TRABAJO Y SEGURIDAD SOCIAL

COMPOSICIÓN*

PRESIDENTE SUBSECRETARIO DEL MTIN

VOCALES UNO O DOS REPRESENTANTES DESIGNADO POR LOS TITULARES DE CADA UNO DE LOS SIGUIENTES ÓRGANOS:

- DOS REPRESENTANTES, SUBSECRETARÍA DE TRABAJO E INMIGRACIÓN.
- DOS REPRESENTANTES, SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL
- DOS REPRESENTANTES, SECRETARIA DE ESTADO DE EMPLEO
- DOS REPRESENTANTES, SECRETARIA DE ESTADO DE INMIGRACIÓN Y EMIGRACIÓN
- UN REPRESENTANTE, DIRECCIÓN GENERAL DE LA INSPECCIÓN DE TRABAJO Y SEGURIDAD SOCIAL
- TITULAR DE LA SUBDIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES (SECRETARIO)

*CON LAS ADAPTACIONES RESULTANTES DE LAS REFORMAS MINISTERIALES LLEVADAS A CABO POR LOS REALES DECRETOS 2/2020, DEL

CUADRO 28

2. POLÍTICA DE USO SEGURO

En esta exposición de las medidas desplegadas en la fase de seguridad, merece especial atención, por su función divulgativa y de concienciación, el documento **"POLÍTICA DE USO SEGURO DE LOS SISTEMAS DE INFORMACIÓN DE LA SEGURIDAD SOCIAL"**.

Se trata de un documento que establece instrucciones y recomendaciones encaminadas a alcanzar la mayor seguridad y eficiencia en el uso de los recursos y sistemas de información de la Seguridad Social, describiendo qué usos se consideran correctos y cuáles indebidos; Informar de las medidas implantadas para el registro del uso y de la finalidad del mismo, y advertir a los usuarios de las consecuencias del incumplimiento de la norma.

Afecta a todo el personal que preste sus servicios para la Seguridad Social entendiendo por "personal" o usuario, a efectos de esta norma, a: los empleados públicos pertenecientes a la Seguridad Social y a los empleados no pertenecientes a la Seguridad Social que utilicen recursos de los sistemas de información de la Seguridad Social.

El documento se estructura en nueve títulos. A continuación se reseña lo más destacable de cada uno de ellos:

INTRODUCCIÓN

Se expone cúal es la finalidad de los sistemas de información de la Seguridad Social, el ámbitro y alcande de la norma, así como las principales siglas, definiciones y referencias.

INSTRUCCIONES GENERALES SOBRE EL USO DE LOS RECURSOS

que aborda, la finalidad del uso de los recursos y sistemas de información, la asignación y retirada de recursos; los principios de sigilo y uso adecuado en la utilización de los recursos, la gestión de la configuración de los ordenadores portátiles, tabletas y teléfonos inteligentes, el deber de colaboración de los usuarios en la comunicación de incidentes de seguridad, así como en facilitar al personal de la unidad TIC competente el cumplimiento de sus obligaciones. Se regulan asimismo las obligaciones de custodiar y no comunicar los elementos de identificación y autenticación que son proporcionados a los usuarios para el acceso a los sistemas informáticos, la obligación de identificación y autenticación de los usuarios, y los que se consideran usos prohibidos.

EL PUESTO DE TRABAJO

En este apartado se establece que los usuarios deben garantizar que la información que muestran los recursos del puesto de trabajo no sea visible a personas no autorizadas y las medidas -bloqueo de la sesión, activación del salvapantallas y apagado- que deben adoptar. Se regulan, también, las características de los soportes de almacenamiento de información, con especial atención a los que contienen datos personales, las actuaciones a seguir en caso de pérdida o sustracción, y la utilización de soportes fuera de las instalaciones de la Seguridad Social. Cómo debe producirse la entrada y salida de datos de las instalaciones de la Seguridad Social, y el control y procedimiento de autorización del uso de interfaces y dispositivos para la entrada o salida de información.

LAS UNIDADES DE ALMACENAMIENTO EN RED

Además de cuestiones generales relativas al almacenamiento en red, se aborda el uso de las unidades o discos locales, el uso que debe realizarse cuando existen unidades de almacenamiento en red compartidas por todos los usuarios (J). Dónde debe almacenarse la información exclusiva del usuario, con diferenciación de si se trata de "uso profesional de la unidad de red exclusiva (H)" o "uso personal de la unidad de red exclusiva" (P), y los usos prohibidos de almacenamiento local o en red.

INTERNET

Se abordan los principios generales bajo los que debe realizarse el acceso a INTERNET, la prohibición del uso de anonimizadores o cualquier otro tipo de software, que pretenda ocultar la navegación del usuario, así como la utilización de dispositivos USB, teléfonos móviles, tabletas (tethering) u otros elementos como acceso alternativo a Internet; el acceso a Internet empleando otro navegador distinto del suministrado y configurado por la GISS en los puestos de usuario. La prohibición de descargar programas informáticos o de ficheros con contenido dañino que supongan una fuente de riesgos para la Seguridad Social, así como el acceso a recursos y páginas web, o la descarga de contenidos que vulneren la legislación en materia de propiedad intelectual o industrial.

CORREO ELECTRÓNICO

En lo referente al uso del correo electrónico se estará a lo dispuesto en la Resolución de 15 de febrero de 2011, de la Secretaría de Estado de la Seguridad Social. Esta disposición regula:

- las figuras que intervienen en el sistema de correo,
- los servicios que comprende el sistema, los procedimientos aplicables para el uso y gestión de los servicios,
- las recomendaciones de buenas prácticas en el uso del sistema del correo, y
- los mecanismos de seguridad adoptados por la GISS en la gestión del uso del mismo.

Como **RECOMENDACIONES DE BUENAS PRÁCTICAS** destacan:

- la utilización de los sistemas de correo corporativo para fines laborales,
- la diferenciación de la cuenta de correo corporativo de la de uso personal,
- no facilitar la dirección de correo corporativo en webs de dudosa confianza,
- evitar dar a conocer la dirección de correo de terceras personas, cuando se envíen copias de un correo a varias personas, con advertencia de que la dirección de correo, al igual que el teléfono es un dato personal.

Especialmente destacable es el apartado dedicado a lo que se considera **ABUSO DEL CORREO ELECTRÓNICO**, en el que se distingue entre la difusión de contenido inadecuado y la difusión masiva no autorizada.

EQUIPOS DE MOVILIDAD

Se establece la diferenciación entre equipos de movilidad personales y corporativos, los principios de acuerdo con los que la GISS lleva a cabo la administración de los equipos y recursos de movilidad, las obligaciones de los usuarios y los usos prohibidos en este tipo de equipos.

REVISIÓN DE USO

Se explicita en este apartado que las actividades de vigilancia y control del uso de los recursos se realizan por la GISS de acuerdo a los principios de idoneidad, necesidad y proporcionalidad. Se especifica bajo qué condiciones se llevará a cabo la revisión del uso: conforme se indica en el **"PROCEDIMIENTO DE REVISIÓN DEL USO DE LOS SISTEMAS DE INFORMACIÓN DE LA SEGURIDAD SOCIAL"**. Se regula el bloqueo o suspensión de los recursos, en caso de que se detecte un uso contrario a lo estipulado en la normativa o cuando no se cumplan los requisitos mínimos de seguridad, y se especifican los recursos cuyo uso se registra, así como los principios que deben regir esta revisión: privacidad y salvaguarda de los derechos fundamentales de los usuarios.

INCUMPLIMIENTO, VIGENCIA E INFORMACIÓN

Se advierte, como cláusula de cierre del documento, de la obligación de respetar las medidas de la **POLÍTICA DE USO SEGURO**, y de las consecuencias del incumplimiento de las mismas. Y se regula la vigencia y la necesidad de difundir el documento a todo el personal.

LA IMPORTANCIA DEL DOCUMENTO PUAS

Constituye el mejor exponente de uno de los dos pilares (seguridad de los sistemas de información y privacidad) a los que se aludía al comienzo de este apartado, concretamente el de la gestión de la seguridad, necesario para que la privacidad de los datos personales manejados por el INSS quede garantizada.

A través de él se consigue llevar a la realidad práctica las políticas y medidas contenidas en el ENS, guiando a través de instrucciones concretas y precisas a todos los usuarios de los sistemas de información de nuestra Entidad hacia un correcto uso de los mismos para salvaguardar no sólo su seguridad sino también la privacidad de los datos personales.

Este documento se encuentra situado en un lugar destacado de la INTRANET, se difunde específicamente al personal de nuevo ingreso en la Entidad y, como se ha señalado en el apartado relativo a la **FASE EXPERIENCIA**, al hablar de los objetivos institucionales adoptados por la Entidad, ha sido objeto de especial atención en los años 2015 y 2016, en los que se estableció un objetivo directamente relacionado con su difusión.

PERFILADO DE LOS USUARIOS

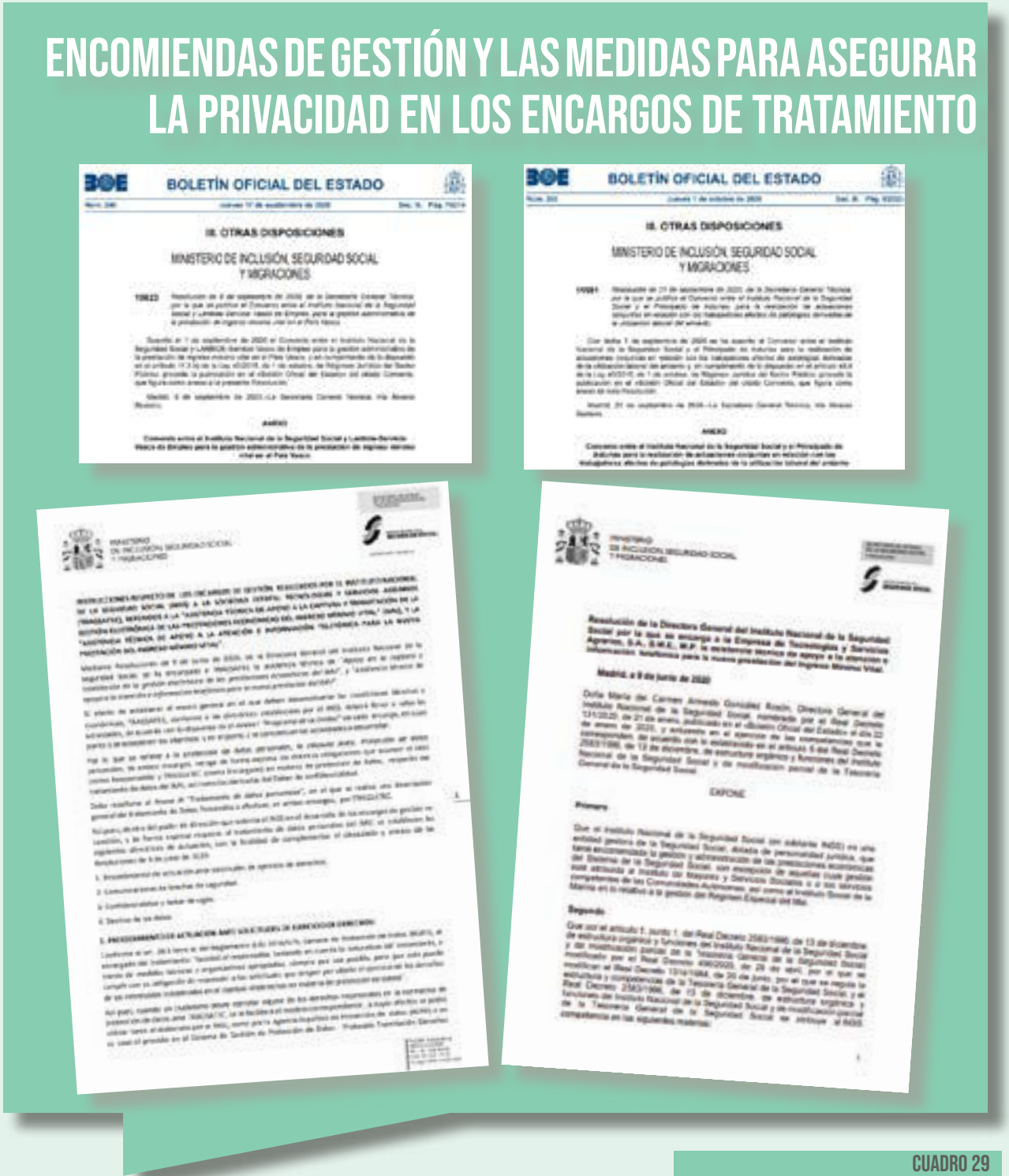
Otro aspecto de seguridad que merece la pena destacarse dentro del amplio abanico de medidas que contemplan nuestros protocolos técnicos es el perfilado de

usuarios. En particular, porque en una organización tan ampliamente descentralizada con una amplia plantilla que trabaja intensivamente con datos personales que incluyen varias categorías especiales de datos, es fundamental e imprescindible prevenir y aplicar la **FILOSOFÍA DE MINIMIZACIÓN Y PRIVACIDAD POR DEFECTO**. De tal forma que esta medida es una pieza fundamental de nuestro sistema sirviendo de garantía de origen para asegurarnos que cada uno de los usuarios sólo pueda acceder a aquello que realmente necesita por las funciones que desempeña.

Todas las bases de datos y herramientas de gestión disponen de un módulo que permite realizar un **PERFILADO GRANULAR** para poder descender a los niveles más concretos y poder determinar, si fuera necesario, un perfilado fino basado en la adecuación a la actividad de cada trabajador y su actualización permanente cuando estas funciones cambien o se produzca una modificación en su adscripción.

El sistema funciona aplicando un **PERFIL DE USUARIO BÁSICO** por defecto que puede enriquecerse con nuevos accesos mediante un sistema de autorización por su superior jerárquico, que además queda acreditada documentalmente. De forma complementaria a todo lo anterior, de todos los movimientos se guarda un historial (*log* de accesos y movimientos) que permite rastrear y realizar labores de **INVESTIGACIÓN INFORMÁTICA FORENSE** si es necesario. Adicionalmente, como se ha explicado ya en otros apartados, se realizan auditorías que seleccionan distintos movimientos a auditar en función de una serie de criterios determinados a nivel estratégico y aplicados por nuestro encargado de tratamiento con competencia en seguridad de los sistemas de información, la **GISS**.

ENCOMIENDAS DE GESTIÓN Y LAS MEDIDAS PARA ASEGURAR LA PRIVACIDAD EN LOS ENCARGOS DE TRATAMIENTO


BOLETÍN OFICIAL DEL ESTADO

III. OTRAS DISPOSICIONES

MINISTERIO DE INCLUSIÓN, SEGURIDAD SOCIAL Y MIGRACIONES

BOLETÍN OFICIAL DEL ESTADO

III. OTRAS DISPOSICIONES

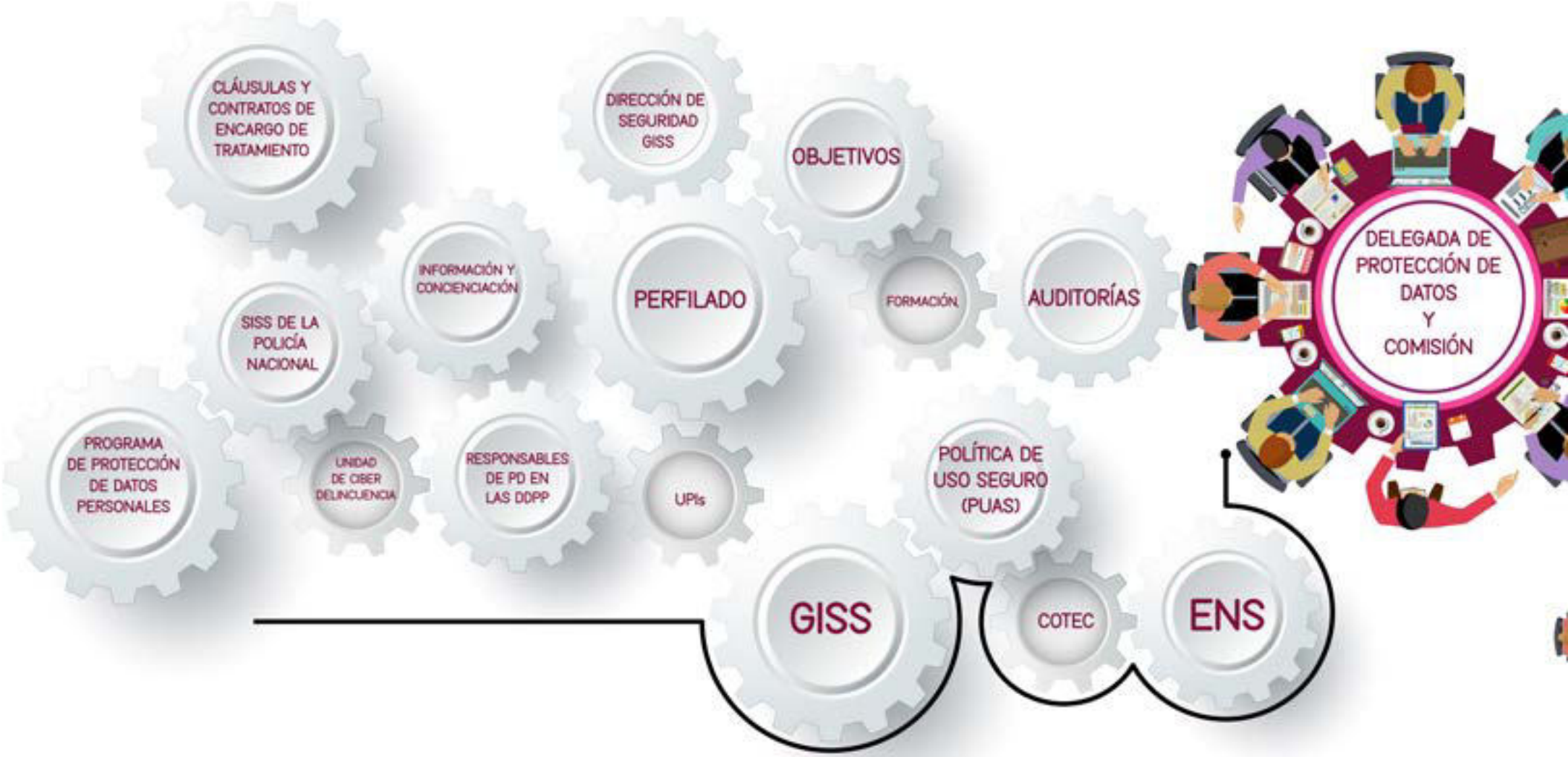
MINISTERIO DE INCLUSIÓN, SEGURIDAD SOCIAL Y MIGRACIONES

Resolución de la Directora General del Instituto Nacional de la Seguridad Social por la que se encarga a la Empresa de Tecnologías y Servicios Agrarios, S.A., S.M.E., M.P. la asistencia técnica de apoyo a la atención e información telefónica para la nueva prestación del Ingreso Mínimo Vital.

EXPONE

CUADRO 29

CUADRO DE LOS DISTINTOS ACTORES EN LA GESTIÓ
Y SUS INTERRELACIONES



ÓN DE LA PRIVACIDAD Y LA SEGURIDAD EN EL INSS

CUADRO 30

En este cuadro **[CUADRO 30]** sintetizamos los **PRINCIPALES ACTORES** que hacen efectiva la privacidad en el INSS a través de las aportaciones en sus respectivos ámbitos: el estratégico, el operativo, el centralizado y el periférico, el centrado en la seguridad de los sistemas y los que aportan el enfoque normativo y el de procesos aplicados a la privacidad. Unos deciden, otros impulsan, hacen o revisan. A través de su perfecto encaje con una relación fluida y bien engrasada armonizada por la persecución de un objetivo común.

Además, a través de la **PARTICIPACIÓN EN EL CSSISS,** y gracias a la instrumentación de la permanente comunicación de todos sus integrantes, los incidentes que afectan a la seguridad de la información o a la imagen y reputación de la Entidad, son trasladados, de manera coordinada por la GISS, a las correspondientes Unidades de Comunicación para su difusión, en su caso, a todos los ciudadanos.

Asimismo, la Entidad, a través de la Inspección de Servicios, pone en conocimiento de la **SECCIÓN DE INVESTIGACIÓN DE LA SEGURIDAD SOCIAL** (SISS), todos los supuestos en los que se detecta la posible comisión de un delito en materia de Seguridad Social, entre otros, aquellos en los que puede verse comprometida la seguridad de los sistemas de información de la entidad – extracción no autorizada de datos- por la intervención maliciosa de terceros. La SISS, cuando en atención a la naturaleza de la actividad delictiva detectada lo considera necesario, da traslado de los hechos a la **UNIDAD DE CIBERDELINCUENCIA.**

3. MEDIDAS DE SEGURIDAD ESTABLECIDAS EN LOS NEGOCIOS JURÍDICOS LLEVADOS A CABO POR EL INSS:

Conforme el artículo 32 del RGPD:

«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».

Es decir, el INSS en su calidad de **RESPONSABLE** de los 43 tratamientos de datos personales en los que se integran la totalidad de los datos, ficheros y sistemas de información en los que se utiliza y custodia los datos personales de los ciudadanos que se realizan con el mismo, está obligado a diseñar e implementar las medidas de seguridad adecuadas para la salvaguarda de la privacidad de los datos personales. Obligación que se extiende a los encargados de tratamientos que en su caso utilice para la gestión de los tratamientos en los que se incluyan los datos.

Para ello, en cada uno de los distintos negocios jurídicos suscritos por el INSS para el adecuado ejercicio de sus competencias, se ha prestado una especial atención al acceso y utilización de los datos personales que se podían ver afectados para establecer las adecuadas cautelas jurídicas en forma de obligaciones jurídicas de obligado cumplimiento, concretizándose las mismas en los siguientes **TIPOS DE NEGOCIOS JURÍDICOS**:

ENCOMIENDAS DE GESTIÓN

En virtud de las cuales, sin producirse cesión alguna de las competencias atribuidas a este Instituto, se acuerda la colaboración con otra administración, incluyéndose las correspondientes cláusulas de protección de datos en la resolución por la que se formalizaban las mismas.

PRIVACIDAD POR DEFECTO EN LOS NEGOCIOS JURÍDICOS

Como se expone en la **FASE NORMATIVA** y **FASE DE GESTIÓN DE LA SEGURIDAD Y LA PRIVACIDAD**, en la formalización de los diferentes negocios jurídicos promovidos por este Instituto se ha prestado una especial atención a las **CLÁUSULAS O DISPOSICIONES DE PROTECCIÓN DE DATOS PERSONALES**, contenidas como parte del contrato de encargo de tratamiento, definiendo las medidas y actuaciones necesarias a realizar tanto por el INSS en su calidad de responsable del tratamiento como por la otra parte compareciente en el negocio jurídico en su calidad de encargada de tratamiento. No obstante, estas medidas que derivarían de la aplicación práctica del principio de privacidad desde el diseño son objeto de una continua revisión y actualización, con el fin de comprobar su adecuada implantación, y analizar si con su implantación se logran los fines perseguidos en cuanto a la protección de datos personales o requieren una nueva reformulación que complementen las disposiciones ya establecidas.

Ejemplo de esta aplicación práctica del principio de privacidad por defecto, es el **ANEXO EN MATERIA DE PROTECCIÓN DE DATOS** establecido para el encargo a medio propio personificado formalizado con la empresa pública TRAGSATEC para la tramitación de la prestación del **INGRESO MÍNIMO VITAL** y su consiguiente tratamiento de datos personales, documento en el que se amplían y desarrollan las medidas establecidas en las cláusulas de protección de datos de la resolución por la que se formaliza el mencionado encargo a medio propio **[ANEXO 9].**

Otro ejemplo sería el **ANÁLISIS DE RIESGO** realizado con posterioridad a la evaluación de impacto en la protección de datos del tratamiento de datos referido al ingreso mínimo vital, ante la necesidad sobrevenida de contratar posteriormente un **SERVICIO DE ALMACENAMIENTO DE SOLICITUDES ELECTRÓNICAS EN LA NUBE [CUADRO 31]**. En el mismo se ha profundizado en los riesgos inherentes a la utilización de dicha tecnología y se han establecido, en colaboración con el responsable de seguridad del INSS a efectos del Esquema Nacional de Seguridad (la Gerencia de Informática de la Seguridad Social), los requisitos de seguridad y privacidad necesarios tanto desde el punto de vista técnico como obligacional, requisitos que han sido incorporados en el correspondiente PCAP como en el pliego de prescripciones técnicas (PPT) del contrato por el cual adjudicar dicho servicio.

CONVENIOS INTERADMINISTRATIVOS PARA LA COLABORACIÓN Y COOPERACIÓN EN EL EJERCICIO DE COMPETENCIAS PROPIAS DE LA ENTIDAD

Donde de forma similar al caso anterior, se incluyen la correspondiente cláusula de protección de datos en el texto del convenio acordado:

CONTRATOS PÚBLICOS

En virtud de los cuales se contrataba la ejecución de una obra, servicio o suministro actuando el INSS en calidad de órgano de contratación y encargado de tratamiento de datos personales, contratos en cuyos pliegos de cláusulas administrativas particulares se han incluido las respectivas cláusulas en materia de protección de datos (Cláusulas 13.7 y 18 del PCAP) **[VEÁSE ANEXO 7].**

ENCARGOS A MEDIOS PROPIOS PERSONIFICADOS

En virtud de los cuales el INSS ejecuta de forma directa (es decir, sin ceder la titularidad de la competencia) una prestación propia de los contratos de obras, suministros, servicios, concesión de obras y concesión de servicios, a cambio de una compensación tarifaria, valiéndose de otra persona jurídica distinta integrada o dependiente del sector público, incluyéndose en la resolución de formalización de los mismos las preceptivas cláusulas de protección de datos **[VEÁSE CUADRO 29].**

4. DESARROLLO DE PROYECTOS ESTRATÉGICOS DE LA ENTIDAD: PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO.

Conforme el **PRINCIPIO DE PROTECCIÓN DE DATOS DESDE EL DISEÑO** cualquier tratamiento de datos personales tiene que cumplir con los requisitos definidos en el RGPD y, por tanto, los derechos de los interesados. Es por ello por lo que debe buscarse que la protección de datos se encuentre presente en las primeras fases de concepción de todo proyecto en el que de soporta al tratamiento de datos.

Estos requisitos se traducen en **MEDIDAS TÉCNICAS Y ORGANIZATIVAS** que persiguen aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento.

La obligación de que se adopten los principios de **PRIVACIDAD DESDE EL DISEÑO** recae en el responsable del tratamiento, con independencia de cual sea la forma de implementación, contratación o adquisición de los medios y técnicas de implantación del tratamiento.

En base a lo anterior, en los distintos proyectos gestados por el INSS se ha prestado una especial atención a la protección de datos personales

ANÁLISIS DE RIESGO Y EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS ASOCIADOS AL INGRESO MÍNIMO VITAL

ANÁLISIS DE RIESGO DEL SERVICIO DE ALMACENAMIENTO EN LA NUBE

EIPD DEL INGRESO MÍNIMO VITAL

CUADRO 31

LA EVALUACIÓN DE IMPACTO DE PROTECCIÓN DE DATOS DEL IMV

RESULTADO DE LA EIPD REALIZADA CON LA APLICACIÓN GESTIONA EIPD

ESQUEMA SINTÉTICO DEL PROCESO DE EVALUACIÓN DE RIESGOS Y MEDIDAS A IMPLANTAR PARA MINIMIZARLOS

CUADRO 32

y la implementación del principio de **PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO**, buscando compaginar de la mejor manera posible las necesidades de gestión y finalidades administrativas a las que el proyecto viene a dar repuesta, con los derechos y obligaciones en materia de protección de datos que se podrían ver afectados a la hora de materializar y ejecutar el mismo.

Como ejemplos más recientes y significativos pueden citarse:

- la creación de la **TARJETA SOCIAL DIGITAL**

El sistema "Tarjeta Social Universal" (denominado hoy Tarjeta Social Digital, TSU/TSD) es un proyecto destinado a **MEJORAR Y COORDINAR LAS POLÍTICAS DE PROTECCIÓN SOCIAL** impulsadas por las diferentes administraciones públicas.

Se trata de un **SISTEMA DE INFORMACIÓN** que integra las prestaciones económicas de carácter social gestionadas por las Administraciones Públicas (Estado, Comunidades Autónomas, Entidades Locales), ya sean pensiones básicas o complementarias, contributivas, no contributivas o asistenciales, prestaciones temporales como los subsidios de incapacidad temporal, nacimiento y cuidado del menor, riesgo durante el embarazo y la lactancia, protección familiar, ingreso mínimo vital, rentas de integración, o prestaciones o ayudas de pago único; en definitiva **TODA PRESTACIÓN SOCIAL DESTINADA A PERSONAS O FAMILIAS**.

En atención a la naturaleza, fines y alcance de este sistema, y en cumplimiento de lo dispuesto en el artículo 35 del RGPD, se realizó una **EVALUACIÓN DEL IMPACTO** de las operaciones de tratamiento necesarias para la articulación de TSU-TSD, en la privacidad de los datos personales.

- y especialmente, el de la prestación económica no contributiva del **INGRESO MÍNIMO VITAL**.

En concordancia con el artículo 35.1 del RGPD: *"Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un*

alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales", por tanto, es el responsable del tratamiento de datos quien debe garantizar que la evaluación de impacto relativa a la protección de datos se realice de forma efectiva y previa a su implantación.

Así pues, para la implantación de esta nueva prestación del Sistema de Seguridad Social creada por el del Real Decreto-ley 20/2020, de 29 de mayo, por el que se establece el ingreso mínimo vital, se realizó la preceptiva **EVALUACIÓN DE IMPACTO DE PROTECCIÓN DE DATOS** del tratamiento de datos que da soporte a dicha prestación (EIPD-IMV).

Para ello se constituyó un **GRUPO DE TRABAJO** con los siguientes integrantes:

1. La Dirección General, como responsable orgánica máxima de la Entidad.

2. La Subdirección General de Gestión de Incapacidad Temporal, prestaciones económicas del sistema de la Seguridad Social en su modalidad no contributiva y otras prestaciones a corto plazo, como responsable funcional del tratamiento y de la prestación.

3. La Secretaría General, dada su doble condición de coordinadora de todas las Subdirecciones Generales, y de SPD del INSS, y en consecuencia, representante y apoyo directo de la DPD de la Seguridad Social.

4. La DPD de la Administración de la Seguridad Social.

Se procedió, de forma previa al inicio de las actividades de gestión, al **ANÁLISIS Y EVALUACIÓN** de:

- el conjunto de actividades destinadas a la captura de datos,
- la clasificación/almacenamiento,
- el uso de dicha información,
- así como de la cesión/transferencia de los datos a un tercero para su posterior tratamiento, y en su caso,
- la destrucción de los mismos,

con la finalidad de poder realizar las actuaciones administrativas necesarias para el reconocimiento, mantenimiento, extinción, control y supervisión del derecho a la prestación del Ingreso Mínimo Vital.

Para ello se hizo una exhaustiva identificación de la totalidad y tipología de datos personales que iban a ser objeto del tratamiento, prestando a una especial atención a los datos personales de carácter especial, y se detectaron los riesgos actuales y potenciales inherentes al uso de los mencionados datos.

Igualmente se identificó a la **PLURALIDAD DE SUJETOS** que de una forma u otra intervenían en la implantación del tratamiento del IMV, para analizar las medidas de seguridad a establecer para paliar los riesgos según el estado de la ciencia y medios razonables disponibles.

Para la evaluación de impacto relativa a la protección de datos del tratamiento del Ingreso Mínimo Vital se ha utilizado la herramienta **GESTIONA-EIPD** de la AEPD, herramienta que guía a su usuario a través de los elementos básicos que deben ser tenidos en cuenta en los análisis de riesgos de los tratamientos y en las evaluaciones de impacto.

GESTIONA-EIPD aporta a responsables y encargados las bases mínimas para iniciar las actividades de análisis y gestión de riesgos en el ámbito del RGPD, incluyendo los requisitos de cumplimiento normativo y medidas encaminadas a reducir o mitigar el riesgo del tratamiento.

GESTIONA-EIPD constituye pues una herramienta de ayuda y soporte a la decisión, cuya utilización genera la documentación básica sobre la cual hay que realizar un análisis y gestión del riesgo por parte de responsables y encargados para cumplir con lo previsto en el RGPD y la LOPDGDD.

Por otro lado, se ha utilizado como modelo para la elaboración del informe, el **MODELO DE INFORME PARA LAS ADMINISTRACIONES PÚBLICAS** elaborado de forma conjunta por la AEPD y la GISS, orientado a cumplir con las previsiones del RGPD incluye, entre las obligaciones del responsable del tratamiento, la necesidad de evaluar el impacto de las actividades de tratamiento en la protección de datos personales cuando resulte probable que el tratamiento suponga un riesgo significativo para los derechos y libertades de las personas.

Este modelo de informe para la EIPD en las AAPP se basa en las siguientes guías y normas:

- La Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD de la AEPD.

- Normas ISO-29134 “Directrices para la evaluación de impacto sobre la privacidad”, ISO-31000 “Gestión del riesgo. Principios y directrices” e ISO-31010 “Gestión del riesgo. Técnicas de evaluación de riesgos”.

Así mismo, se ha tenido en cuenta el listado de tratamientos en los que es obligatorio realizar una evaluación de impacto publicado por la AEPD, y conforme el cual resulta de obligado cumplimiento el realizar la presente **EVALUACIÓN DE IMPACTO PARA EL TRATAMIENTO DEL INGRESO MÍNIMO VITAL**. En este caso los **SUPUESTOS PRINCIPALES** que han motivado su realización han sido:

1. Tratamientos que impliquen el uso de **CATEGORÍAS ESPECIALES DE DATOS** a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.

EJEMPLO DE PRIVACIDAD POR DEFECTO Y EL PRINCIPIO DE MINIMIZACIÓN DE DATOS

INFORME MÉDICO DE SÍNTESIS CON DATOS MÉDICOS COMPLETOS ACCESIBLE PARA EL PERSONAL DEL EQUIPO DE VALORACIÓN DE INCAPACIDADES (EVI)

INFORME MÉDICO DE SÍNTESIS CON DATOS MÉDICOS OCULTOS ACCESIBLE PARA LA INTERVACIÓN Y TERCEROS CON DERECHO DE ACCESO AL EXPEDIENTE

CUADRO 33

2. Tratamientos que impliquen la **ASOCIACIÓN, COMBINACIÓN O ENLACE DE REGISTROS DE BASES DE DATOS** de dos o más tratamientos con finalidades diferentes o por responsables distintos.

3. Tratamientos de datos de **SUJETOS VULNERABLES O EN RIESGO DE EXCLUSIÓN SOCIAL,** incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia.

En cuanto a **NORMATIVA** de obligado cumplimiento, se ha tenido en cuenta:

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Por último, deben señalarse, además, las medidas de **PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO** aplicadas al tratamiento del ingreso mínimo vital, implementadas en las distintas fases del tratamiento donde se han tenido en cuenta, en particular, la Guía de Privacidad desde el Diseño publicada por la AEPD, y en general, las guías y notas publicadas en la web de la AEPD en el apartado Innovación y tecnología.

En cuanto a las **MEDIDAS DE SEGURIDAD** se han establecido las medidas establecidas por la Gerencia de Informática de la Seguridad Social (GISS) para garantizar el cumplimiento de los requisitos establecidos por el **ESQUEMA NACIONAL DE SEGURIDAD**, analizando los requisitos necesarios para minimizar los riesgos para los derechos y libertades sobre los dominios de seguridad:

En resumen, teniendo en cuenta que quedan salvaguardados en todo momento los derechos y libertades de los ciudadanos afectados por su implantación, en el ámbito de la protección de datos personales, como de la protección social, tanto en la vía administrativa, como jurisdiccional, se ha concluido un balance riesgo-beneficio positivo a favor de la implantación del tratamiento del ingreso mínimo vital, con las medidas correctoras y de seguridad expuestas, tal como ha concluido la EIPD realizada del mismo, a través de la herramienta de la AEPD, **GESTIONA_RGPD [CUADRO 32).**

Por último, debe destacarse que la participación en los proyectos de la entidad para ver la incidencia de los mismos en el ámbito de la protección de datos se hace desde una perspectiva dinámica, realizándose una labor continua de supervisión y actualización de las medidas de protección de datos en función de las circunstancias de cada momento.

Como ejemplo puede referenciarse, lo ya comentado en otra apartado, en relación al **ANÁLISIS DE RIESGOS** efectuado para la contratación del servicio de almacenamiento en la nube de las solicitudes del ingreso mínimo vital, en el cual, se han detectado y analizado los riesgos y se han diseñado en implementado las medidas paliativas acordadas para evitar los riesgos que contrae la contratación y utilización de dicho servicio de almacenamiento.

Como ejemplo del seguimiento por parte de la Entidad del principio de privacidad por defecto y materializando el principio de minimización de datos, se muestra en el **CUADRO 33** las dos versiones del documento **INFORME MÉDICO DE SÍNTESIS** donde se recoge el diagnóstico considerado en la evaluación de la incapacidad laboral del interesado, sólo en el supuesto de que el destinatario del mismo tenga la condición de interesado en el procedimiento administrativo.

FASE
CONTROL Y REVISIÓN

Como última parte del **PROCESO DE TRANSFORMACIÓN** que se describe a lo largo de esta memoria, ocupa una posición muy relevante aquella que cierra cada ciclo de iteraciones para conseguir una plena implantación del **ENFOQUE 360°** a todos los niveles de la organización, siendo la pieza de cierre de cada ciclo y de apertura del siguiente, a través del que se incrementa nuestro aprendizaje y con el que continuamos identificando oportunidades de mejora y buenas prácticas que mantener y exportar a otros ámbitos de la gestión o nuevos proyectos, tal y como se mostraba esquemáticamente en el **CUADRO 5** de Factores clave del proceso de adaptación.

Dentro de esa fase se engloban, entre otras, las actuaciones que se desarrollan a continuación:

PROGRAMA DE INSPECCIÓN DE PROTECCIÓN DE DATOS

Las visitas de inspección son una importante fuente de conocimiento real de cómo se traducen en la práctica las actividades que se encuadran en la **FASE NORMATIVA** y permiten comprobar el grado de éxito y efectividad tienen aquellas otras actividades incluidas en la **FASE PLANIFICACIÓN** y en la **FASE DE ACCIÓN**.

También suponen una fuente de conocimiento de cuáles son las áreas que hay que reforzar a nivel de formación e información, con lo que sirven para nutrir la **FASE DE GESTIÓN DEL CONOCIMIENTO** y contribuyen a ella a través de la labor pedagógica que se realiza en estas visitas.

Por último, hay que tener en cuenta que también son un importante instrumento para **TOMAR EL PULSO DE LA EFECTIVIDAD DE LAS MEDIDAS DE SEGURIDAD IMPLANTADAS** y de cómo su implantación impacta en la gestión.

Por ello, este programa es una pieza clave en el **FLUJO DE CONTROL Y REVISIÓN,** que se proyecta incluso en su propio ámbito, pues el programa de protección de datos se autoenriquece con la experiencia y aprendizaje que se deriva de cada visita y su contenido se encuentra en constante revisión y actualización, para mantener su efectividad y ampliar su radio de acción a las nuevas áreas de actuación que se van desarrollando.

En el caso de este programa, ya se han completado en algún supuesto **HASTA TRES VISITAS EN CADA PROVINCIA**, lo que permite hacer seguimiento de la actividad provincial y conocer de primera mano su evolución en la materia **[CUADRO 7].**

OBJETIVOS INSTITUCIONALES

Tal y como se apuntado en la descripción general del proceso de adaptación llevado a cabo por el INSS, la entidad ha actuado siguiendo los principios y esquemas lógicos del modelo EFQM, que exigen, tras la planificación de los resultados a alcanzar, la determinación del enfoque que se considera más apropiado para ello, y la realización del despliegue en las áreas más relevantes: la **EVALUACIÓN Y REVISIÓN** de los resultados alcanzados, en una constante tarea de mejora continua en el cumplimiento de las medidas de privacidad de los datos.

Siguiendo esta dinámica, la Secretaría General, con el asesoramiento del GPTD que asiste a la SPD, analiza y valora la oportunidad de establecer nuevos objetivos institucionales adecuados al nivel de desarrollo de la política de privacidad.

En esta línea, se está trabajando en la concreción de un **OBJETIVO PARA EL AÑO 2021,**

dirigido a garantizar que las instrucciones sobre protección de datos enviadas por la Secretaria General han sido objeto de actuaciones específicas por las DDPP, con vistas a su conocimiento por todo el personal de cada centro.

Cuando finaliza el periodo en el que ese objetivo debe cumplirse, se procede a **REVISAR SU GRADO DE CUMPLIMIENTO**, lo que puede servir de una forma de valoración global a nivel de la entidad del **"ESTADO DE SALUD"** de esa materia. Por otra parte, los objetivos también se revisan y modifican para mejorar y ampliar su ámbito de acción, en función del grado de efectividad de las actuaciones realizadas y el grado de complejidad que haya supuesto para las distintas provincias al realizarlas.

PERFILADO

En este caso concreto, el último objetivo diseñado, como ya se ha desarrollado en otros apartados anteriores, dada la importancia de esta **FASE DE CONTROL Y REVISIÓN**, tiene como finalidad precisamente reforzar el proceso de control y revisión en el ámbito periférico con la intención de completar un ciclo íntegro análisis de la adecuación del perfilado de acceso a transacciones de toda la plantilla.

AUDITORIA

Otro pilar fundamental de esta fase son los procesos de auditoria a todos los niveles en los que tiene impacto la política de privacidad.

De la misma manera, los principios de mejora continua imprimen al proceso de auditorías, una **DINÁMICA DE CONTINUA REVISIÓN**, de manera que se incorporan al sistema nuevos supuestos y actuaciones dirigidas a verificar la adecuación de los accesos a los datos de la Entidad.

Así, como ejemplo, en los convenios suscritos recientemente por el INSS para la gestión administrativa de la prestación de ingreso mínimo vital (IMV) se establecen cláusulas que imponen al organismo que conviene con el INSS, la obligación de poner a su disposición toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del INSS o de otro auditor autorizado por dicho responsable.

La Unidad Nacional de Auditorías, en colaboración con los responsables del tratamiento IMV está revisando el proceso de auditorías a realizar en estos supuestos.

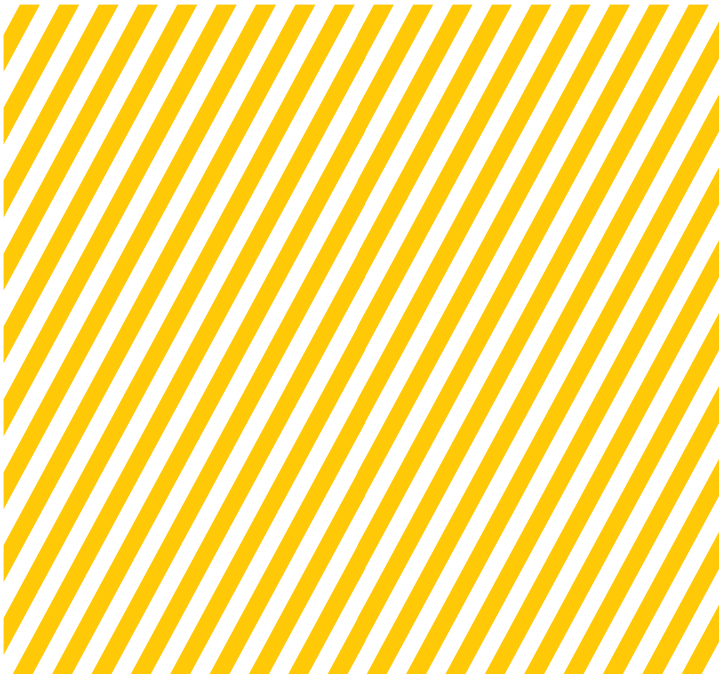
MAPA DE LA PROTECCIÓN DE DATOS DEL INSS

Por la importancia que se da a esta fase, durante todo el proceso de transformación se está recabando la información necesaria para construir una verdadera cartografía de la privacidad en nuestra entidad. Una vez completado facilitará todos los procesos de revisión, al tener localizados todos los puntos que deberían ser objeto de actualización en cualquier supuesto de cambio normativo o cualquier otra actuación que así lo requiriese, incluidos el análisis y la toma de decisiones estratégicas.

Este gran mapa, asimismo también deberá ser objeto de actualización permanente para proporcionar datos precisos y fiables en todo momento.

GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS

El GTPD constituye no sólo una pieza clave de la fase de acción sino un auténtico **INSTRUMENTO DE CONTROL Y REVISIÓN**, a través de sus reuniones periódicas y las actuaciones que en ellas se acuerdan y revisan. Su labor es muy relevante porque al contar con representantes de todos los ámbitos de la organización permite tener una visión global y por áreas, que redunda en el avance hacia ese enfoque 360º que perseguimos. A través de su labor y la que realizan de forma periférica los interlocutores o representantes provinciales de protección de datos se consigue **TENER "OJOS" Y CAPACIDAD DE ACCIÓN** en todos los ámbitos, también a efectos de los flujos de control y revisión que ahora analizamos.



TRES EJEMPLOS DE BUENAS PRÁCTICAS EN LA PROTECCIÓN DE DATOS

LA PRIVACIDAD Y LOS TRATAMIENTOS DE DATOS DE VIOLENCIA DE GÉNERO EN EL INSS

La violencia de género y cualquier otra forma de violencia contra la mujer se combate de manera integral por el conjunto de los poderes públicos.

Es por ello por lo que en la Seguridad Social se han dispuesto de una serie de medidas tendentes a paliar los efectos sufridos por las víctimas en estas situaciones de violencia, ya sea por las propias mujeres como también por sus hijos.

Entre esas medidas se encuentran:

Garantías en forma de consideración de determinados periodos como cotizados a efectos de acceso a prestaciones, en materia de de pensión de viudedad en casos de separación, divorcio o nulidad matrimonial, de la forma de acceso al derecho a la asistencia sanitaria, a la jubilación anticipada involuntaria o respecto de la pensión de orfandad para las hijas e hijos de víctimas de violencia de género y otras formas de violencia contra la mujer.

Así como el impedimento para que el agresor sea beneficiario de prestaciones o pueda serle abonada la pensión de orfandad a los hijos.

Como resultado de esa especial cobertura, el INSS debe tratar los datos personales de las víctimas para gestionar esas solicitudes y las posibles prestaciones que de ellas se deriven. Así, en la actualidad se gestionan más de 6000 expedientes de muerte y supervivencia con un componente de violencia de género en ellos.

ESPECIAL PROTECCIÓN DE DATOS PERSONALES EN LOS SUPUESTOS DE VIOLENCIA DE GÉNERO

La Seguridad Social limita en todo caso el acceso y utilización de los datos personales, con especial atención a las víctimas de violencia de género o en el ámbito familiar. Además, las víctimas de violencia contra la mujer pueden solicitar, a través de nuestras Oficinas de la Seguridad Social, así como a través del registro electrónico, que el acceso a sus datos quede especialmente limitado y controlado.

Para ello se aprobó el "Procedimiento de actuación conjunta entre las entidades:

- Tesorería General de la Seguridad Social (TGSS),
- Instituto Nacional de la Seguridad Social (INSS), e
- Instituto Social de la Marina (ISM),

para la especial protección de los datos de las personas que así lo hubieran solicitado", en base al cual se procede al **BLOQUEO/OCULTACIÓN** de los expedientes y datos personales de las personas que lo soliciten. En estos casos, esos datos sólo podrán ser consultados por los funcionarios que ostenten una elevada responsabilidad en sus unidades y hayan sido autorizados para ello. En el resto de casos, ni siquiera por error (seguridad por defecto y principio de minimización de datos), podrían ser consultados por otros empleados de la organización.

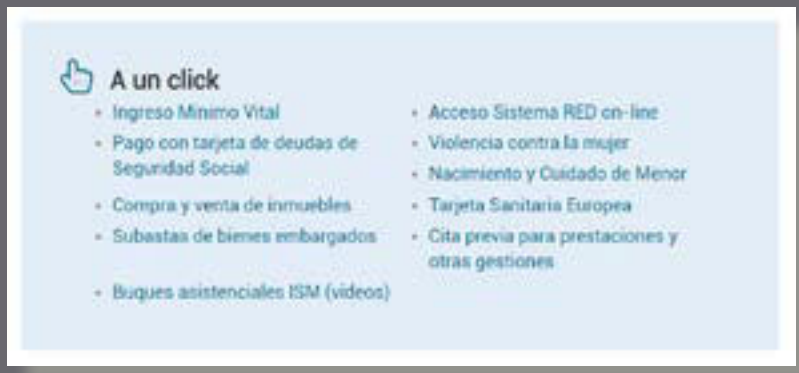
Así mismo, se recoge de forma expresa en la Instrucción Segunda del documento **"INSTRUCCIONES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES PARA LA GESTIÓN ORDINARIA DE LA ACTIVIDAD PRESTACIONAL Y EL RÉGIMEN INTERNO DEL INSTITUTO NACIONAL DE LA SEGURIDAD SOCIAL"** (VER ANEXO 6) donde se fijan unas concretas pautas de actuación para los empleados de la Entidad en este supuesto particular.

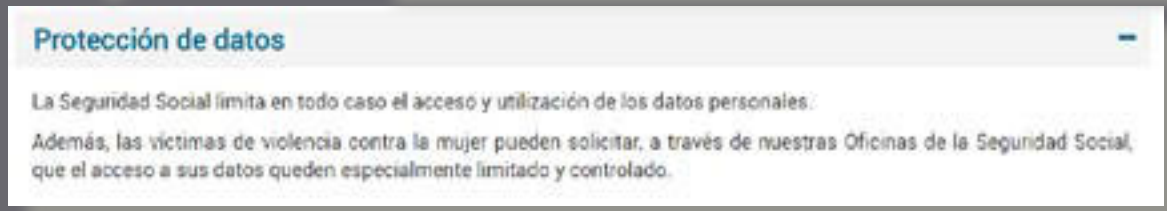
Otra medida de seguridad adicional es que los expedientes de esta naturaleza se conservan en la denominada **CARPETA DE DATOS SENSIBLES**, con especiales garantías en cuanto a su acceso, de nuestra aplicación de gestión documental SARTIDO. De esta forma, nos aseguramos de que esa información no sea accedida mas que por aquellos funcionarios especialmente autorizados para ello, extremando así las garantías de seguridad para estas personas.

OTRAS MEDIDAS DE CONCIENCIACIÓN Y MEDIDAS PARA EL CORRECTO TRATAMIENTO DE DATOS RELACIONADOS CON LA "VIOLENCIA DE GÉNERO".

En la Intranet de nuestra entidad se incluyen contenidos destinados a concienciar e informar en la materia, e incluso, facilitar otras herramientas como las que se contienen en el apartado de "Protección de Datos Personales" de la **INTRANET** del INSS, donde se han indexado diferentes documentos y enlaces seguros (no dejan rastro de navegación) a las principales web y administraciones de ayuda a las mujeres víctimas de este tipo de violencia para que tengan un fácil acceso a este tipo de información.

Por otra parte, en la **PÁGINA WEB** de la Seguridad Social se dedica un apartado especialmente dedicado a la materia de la violencia de género y las prestaciones asociadas a ellas que gestiona este Instituto. Esta información tiene un acceso destacado en el apartado "a un click" de la pantalla inicial.





OTROS DATOS PERSONALES QUE RECIBEN UNA ESPECIAL PROTECCIÓN

Relacionado con lo anterior, también disponemos de **PROTOCOLOS DE ACTUACIÓN FRENTE AL ACOSO LABORAL, SEXUAL Y POR RAZÓN DE SEXO**, que además de recoger el compromiso institucional de la Administración para prevenir y en su caso erradicar las situaciones de acoso que se pueden desarrollar con ocasión del desempeño de la actividad laboral, se tiene en cuenta la necesaria protección de los datos personales que se deriven de estas actuaciones.

En particular, la Subdirección General de Recursos Humanos de la Entidad presta una especial atención a dichas situaciones, siempre con el auxilio de la Inspección de Servicios del INSS, que realiza esta labor con la máxima reserva y garantías de confidencialidad.

EL TRATAMIENTO DE LOS DATOS PERSONALES DE SALUD EN EL INSS Y LAS GARANTÍAS PARA SU PRIVACIDAD

38.669.336 ACCESOS A DATOS MÉDICOS A TRAVÉS DE ATRIUM EN **2019**

4.115 USUARIOS APLICACIÓN ESPECÍFICA DE GESTIÓN DE UNIDADES MÉDICAS ATRIUM

946.925 PENSIONES DE INCAPACIDAD PERMANENTE ACTIVAS

8.019.281 PARTES MÉDICOS TRANSMITIDOS

190.419 RECONOCIMIENTOS MÉDICOS EFECTUADOS

889.550 PROCESOS DE **IT** ACTIVOS

831 OTROS PROCESOS: RIESGOS DURANTE EL EMBARAZO/LACTANCIA Y CUIDADO DE MENOR AFECTADO DE CÁNCER U OTRA ENFERMEDAD GRAVE

12.881 AFECTADOS DEL SÍNDROME TÓXICO

INCIDENCIA DE LOS DATOS DE SALUD EN LA GESTIÓN DEL INSS

Algunas de las competencias más destacables del INSS se basan en los tratamientos intensivos de datos personales de carácter médico en el sentido amplio que dibuja el actual RGPD. Es el caso de la **INCAPACIDAD TEMPORAL** y la **INCAPACIDAD PERMANENTE**, principalmente, si bien, existen otras prestaciones en las que también deben tenerse en cuenta la evaluación de la situación médica o de salud de sus beneficiarios o causantes: riesgo durante el embarazo o la lactancia natural, cuidado de hijos o menores a cargo afectados de cáncer u otra enfermedad grave, prestaciones sanitarias del seguro escolar, recargo por falta de medidas de seguridad en el trabajo, síndrome tóxico, asistencia sanitaria en el extranjero, algunos tipos de pensiones de orfandad e incluso de jubilación cuando se dan unos supuestos específicos de discapacidad derivados de una lista de enfermedades tasadas reglamentariamente.

ACCESO AL HISTORIAL MÉDICO DE LOS

SERVICIOS PÚBLICOS DE SALUD

Para algunas de las prestaciones anteriores se dispone de **ACCESO AL HISTORIAL MÉDICO DE LOS SERVICIOS PÚBLICOS DE SALUD** de los interesados para poder hacer las evaluaciones de su estado de salud y su posible incapacidad laboral, en otros casos, esta documentación es aportada por los propios interesados en diversos formatos (físicos, magnéticos, otros).

UNIDADES DE VALORACIÓN MÉDICA DE INCAPACIDADES

En una parte de las prestaciones puede ser necesaria una **EVALUACIÓN PRESENCIAL** de los solicitantes o perceptores de prestaciones, lo que se efectúa en unas dependencias específicas, las **UNIDADES DE VALORACIÓN MÉDICA DE INCAPACIDADES** (UVMI) que existen en todas las direcciones provinciales salvo las correspondientes a Cataluña que tienen un régimen de gestión diferenciado en esta materia.

Un **HITO** de relevancia en estas UVMI es la instalación de sistemas inteligentes de espera que **SALVAGUARDAN LA IDENTIDAD DE LOS INTERESADOS** que son citados para evitar tener que usar su nombre y apellidos para ser llamados al despacho del inspector médico, todo ello en cumplimiento de la Ley 41/2002, de 14 de noviembre básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica y como resultado del programa de inspección específico que se realizó sobre unidades médicas y protección de datos. En estos momentos, en todas las dependencias de las UVMI del Estado se garantiza el anonimato de las personas que son llamados a cita.

EQUIPOS DE VALORACIÓN DE INCAPACIDADES

Por otra parte, otra peculiaridad en el tratamiento de estos datos personales, es la celebración periódica de reuniones de los **EQUIPOS DE VALORACIÓN DE INCAPACIDADES** (EVI o Comisión de Evaluación de incapacidades, CEI en el caso de Cataluña). Estos equipos son multidisciplinares e incluyen a personal externo a la organización, como pueden ser inspectores de trabajo.

En estas sesiones, hasta hace unos años todas las valoraciones se hacían basándose en la documentación obrante en papel, incluida la que contenía datos médicos, lo que dificultaba enormemente la gestión de la protección de estos datos, al ser necesarias la implantación de medidas de seguridad que afectaban de forma notable a la gestión restándole mucha agilidad.

Por ello, en las **VISITAS DE INSPECCIÓN** del programa de protección de datos se prestaba especial atención a esta circunstancia, a la forma en la que se producían los desplazamientos de documentación y las garantías que ésta ofrecía. A la vista de lo observado se consideró oportuno promover formas alternativas de gestión de estas sesiones que dejaran de lado el formato papel para convertirse en **SESIONES ELECTRÓNICAS** que se basaban en la consulta de las aplicaciones o carpetas digitales donde se guardaba la documentación.

Con la progresiva implantación de estas nuevas tecnologías se ha ido mejorando de forma notable la seguridad de esta información especialmente sensible y los procesos asociados a la gestión documental en formato no electrónico, reduciendo significativamente los tratamientos de esta naturaleza que aún se realizaban en formato papel.

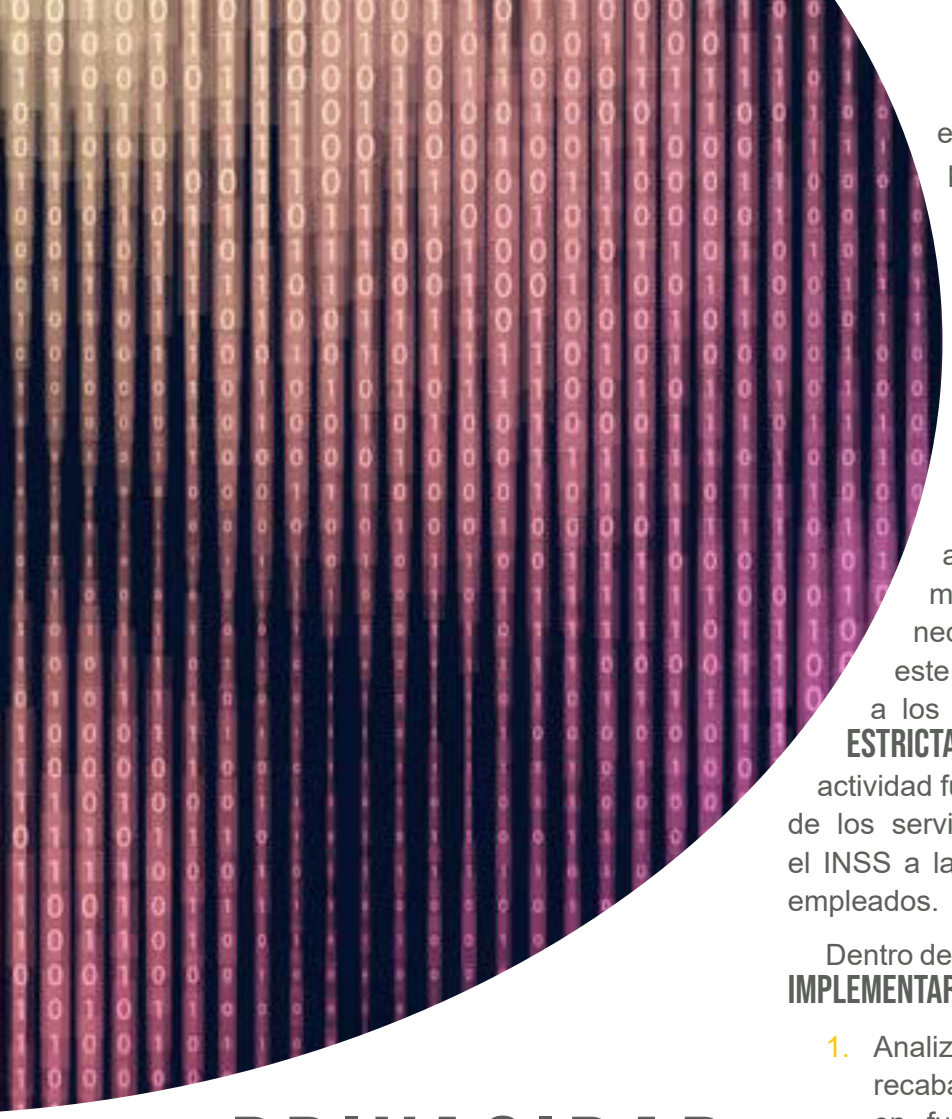
GESTIÓN DOCUMENTAL ELECTRÓNICA

En cuanto a la **GESTIÓN DOCUMENTAL ELECTRÓNICA**, la herramienta corporativa del INSS es SARTIDO, apliación y modelo de gestión al que dedicamos otro apartado monográfico por su gran importancia y trascendencia en el ámbito de la gestión, eliminación de cargas burocráticas, pero también, sin duda, de la adecuada protección de los datos personales, en particular, de aquellos que se consideran más sensibles, como son los de salud.

En esta aplicación, además de existir una carpeta de documentación sensible a la que ya se hizo referencia en el apartado dedicado a la protección de datos de las personas víctimas de violencia de género, existe otra **CARPETA MÉDICA** específica para conservar los datos de salud de forma diferenciada al resto de los documentos que se conservan en la herramienta. Todo ello con el propósito de dispensar una mejor seguridad al permitir el perfilado de acceso y aplicar otros mecanismos de control a esa carpeta de forma diferenciada del resto y la aplicación de medidas de seguridad de la información más robustas que en el resto de casos.

INSTRUCCIONES

Por último, mencionar que para dar cumplimiento a las mayores garantías de seguridad también se dictan instrucciones sobre el correcto manejo de estos datos.



PRIVACIDAD POR DEFECTO EN LA GESTIÓN DOCUMENTAL

La privacidad por defecto requiere el revisar y analizar las políticas de privacidad implantadas, especialmente en lo que se refiere al principio de minimización de datos y la confidencialidad y seguridad de los datos personales. Ello supone el compartimentar el uso del conjunto de datos entre los distintos tratamientos, de tal forma que no todos los tratamientos accedan a todos los datos, sino que actúen solo sobre aquellos que sean necesarios y en los momentos en que sea estrictamente necesario. Por eso los empleados de este Instituto sólo han de tener acceso a los datos de carácter personal que son **ESTRICTAMENTE NECESARIOS** para realizar su actividad funcionarial/administrativa en la gestión de los servicios y procedimientos ofertados por el INSS a la ciudadanía, así como a sus propios empleados.

Dentro de las posibles **ESTRATEGIAS QUE PERMITEN IMPLEMENTAR LA PRIVACIDAD POR DEFECTO** destacan:

1. Analizar los tipos de datos que se están recabando con un criterio de minimización en función de los productos y servicios solicitados por los ciudadanos;
2. Analizar los procesos asociados a dichos tratamientos para que se utilicen los mínimos datos personales necesarios para ejecutarlos;
3. Revisar la política de conservación de datos desde un punto de vista restrictivo, eliminando aquellos datos que no sean estrictamente necesarios;
4. Limitar el acceso por parte de terceros a dichos datos personales.

Actuaciones que se han traducido en medidas tanto técnicas como organizativas.

Mediante Resolución de 14 de noviembre de 2007, del Instituto Nacional de la Seguridad Social, por la que se aprueba la aplicación informática del sistema de almacenamiento, recuperación, tratamiento de imágenes y documentos ofimáticos (SARTIDO), se instauró dicha aplicación informática para efectuar el tratamiento de la información necesaria para la generación y archivo de documentos electrónicos a partir de la documentación suministrada en soporte papel, tanto por los ciudadanos, como por las administraciones y resto de sujetos con los que se interrelaciona este Instituto en su actividad administrativa.

Este aplicativo informático presenta tres grandes funcionalidades en las que se pone de manifiesto la privacidad por defecto, como son:

- **MÓDULO DE GESTIÓN DOCUMENTAL**:

genuino gestor documental (archivo electrónico) que permite la digitalización de la documentación y su archivo electrónico. Dada la complejidad y pluralidad de tipología documental que es custodiada por el INSS (documentación médica, sentencias judiciales especialmente sensibles: violencia contra la mujer, violencia en el ámbito doméstico, explotación sexual, trata de seres humanos, maternidad por subrogación, etc.), el mismo se ha estructurado bajo la premisa de una arquitectura compartimental funcional que permita minimizar al máximo los riesgos

inherentes a la utilización y custodia de la información, sin entorpecer o imposibilitar la gestión administrativa o los derechos sociales de los ciudadanos.

Así pues, para cada tipo de prestación de carácter social competencia de este Institutito, se han establecido 19 compartimentos (carpetas electrónicas) en las que indexar la documentación en función de la información que aporta, lo cual permite controlar y restringir tanto el acceso a las mismas, como las funcionales posibles (visualizar, copiar, imprimir, indexar, eliminar). De esas 19 carpetas electrónicas, 3 son objeto una **ESPECIAL PROTECCIÓN**, restringiéndose al máximo los controles de acceso **(CUADRO 34)**:

- 03-Documentación Médica y EVI:

documentación médica del expediente, tanto la aportada por el ciudadano como la generada por las aplicaciones corporativas, trámite y su gestión.

- 06-Sentencias:

Documentación relacionada con demandas y sentencias para el trámite administrativo en las que el INSS sea parte o interesado.

- 17-Documentación sensible:

Documentos con datos de carácter personal (por ej. Denuncias, sentencias o documentación que acrediten la condición de víctima de violencia de género, datos relativos a menores, sentencias de divorcio, documentación relativa los trámites de adopción o maternidad por subrogación, etc.) y que no se incluyan en la carpeta 03-Documentación médica y EVI, ni 06-Sentencias.

Dada la repercusión directa en la protección de datos personales que los ciudadanos que presenta esta funcionalidad del aplicativo SARTIDO, es objeto prioritario de la política de privacidad de este Instituto, tal como lo demuestra el que constituya la primera de las Instrucciones en materia de protección de datos dictadas al conjunta de las 52 Direcciones Provinciales del INSS (INSTRUCCIÓN PRIMERA. Digitalización y archivo electrónico de la documentación **(ANEXO 6**).

MÓDULO DE REGISTRO:

es una funcionalidad diferenciada del gestor documental que permite asignar un registro interno a la totalidad de la documentación que se indexa en el aplicativo SARTIDO, ya sea con destino u origen en el mismo, estando interconectada con el registro electrónico de la Entidad y la Sede Electrónica de la Seguridad Social.

MÓDULO DE NOTAS:

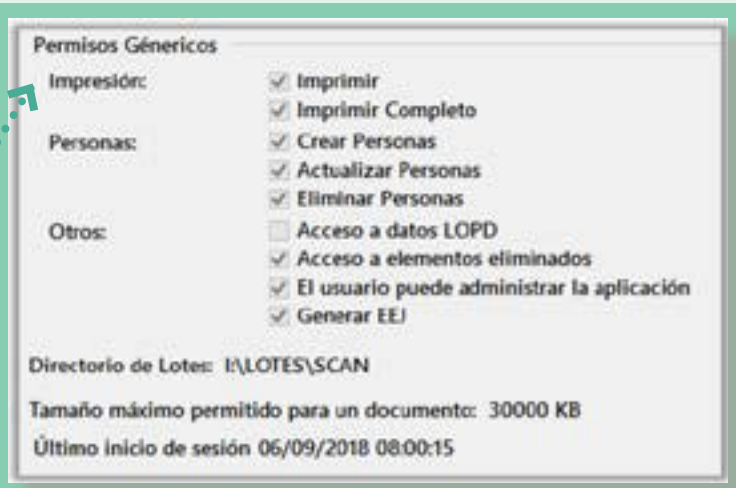
se trata de una funcionalidad que permite el envió y recepción de notas internas del Instituto, adjuntándose a la mismas la documentación requerida a través de estas con plena validez jurídica en cuanto a formalidades de firma electrónica o requisitos similares.

Dada la importancia que tienen los documentos y datos que a través de estas funcionalidades se conservan o transmiten, los accesos ea cualquiera de los 3 módulos funcionales descritos, necesariamente se han estructura de forma que se permita un correcto **PERFILADO (CUADRO 34)**, selectivo de las unidades y funcionarios adscritos a las mismas.

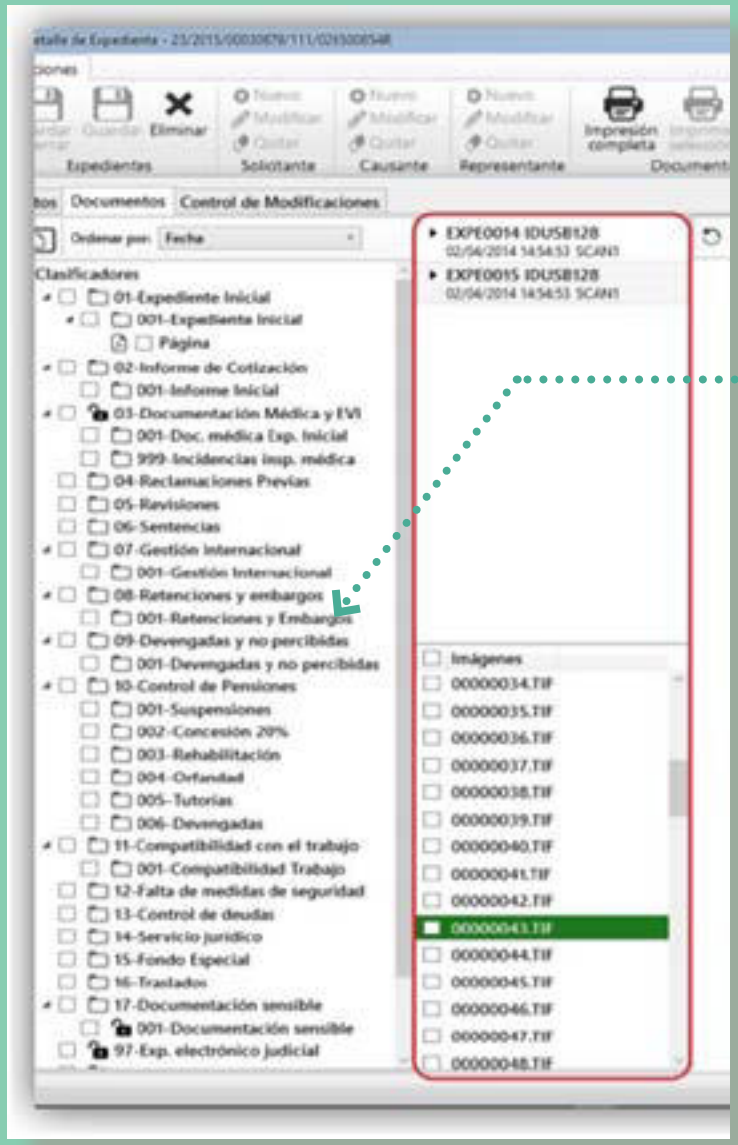
Asimismo, en atención a las distintas acciones a las que los empleados de esta entidad quedan autorizados en relación a las funciones concretas de supuesto de trabajo, se ha buscado el potenciar al máximo la disponibilidad, integridad, confidencialidad, accesibilidad y protección de la información integrada en los documentos utilizados por el aplicativo, **REVISÁNDOSE Y AUDITÁNDOSE** de forma periódica los perfiles atribuidos a los distintos usuarios, así como la arquitectura de unidades orgánicas establecidas, minimizándose con ello los riesgos existentes.

PERFILADO Y SISTEMA DE CONSERVACIÓN DE LA DOCUMENTACIÓN ELECTRÓNICA

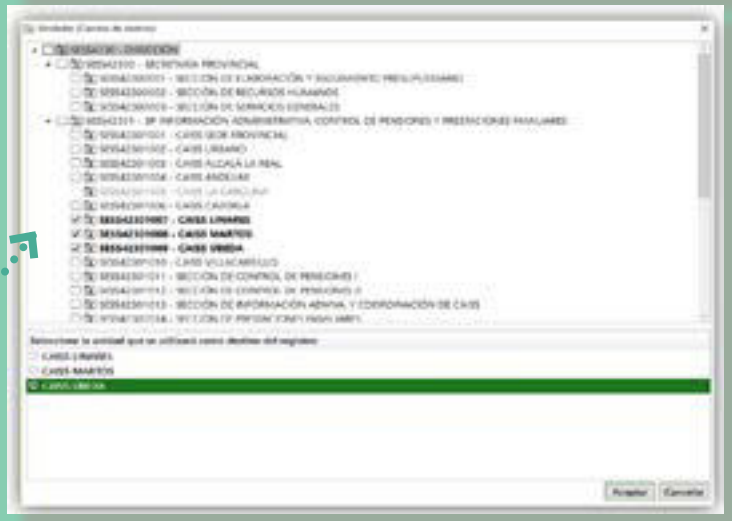
TIPO DE PERMISOS



DETALLE DE UN ÁRBOL DE UN EXPEDIENTE EN SARTIDO



MÓDULO DESTINATARIOS DE NOTAS



CARPETAS DEL MÓDULO DOCUMENTAL

REFLEXIÓN FINAL

El camino de la adaptación que en esta memoria describimos, empezó mucho antes de que tomáramos verdadera conciencia de ello, mucho antes de que el nuevo Reglamento fuera siquiera un proyecto. Esa andadura previa configuró nuestra forma de entender el universo de la protección de datos desde la conciencia del camino que teníamos por delante, el inconformismo y el compromiso con los ciudadanos y los empleados de la organización; buscando nuevos horizontes para mejorar la privacidad de los datos de los ciudadanos y empleados que los confían a nosotros. A partir del primer esbozo del Reglamento, ese camino tomó un nuevo rumbo más exigente, proactivo y sabio, uno que es difícil precisar dónde comienza pero imposible determinar dónde acaba pues la empresa que a los equipos que colaboran en hacer realidad el enfoque 360º y una privacidad efectiva y plena, se les ha encomendado es una apasionante labor sin fin.

"Los límites son para aquellos que los necesitan"


INSTITUTO NACIONAL DE LA
SEGURIDAD SOCIAL